Network Protocol Configuration Commands

Table of Contents

Chapter 1 IP Address Configuration Commands

1.1 IP Address Configuration Commands

IP Address Configuration Commands include:

- arp
- arp timeout
- clear arp-cache
- ip address
- ip directed-broadcast
- ip forward-protocol
- ip helper-address
- ip host
- ip proxy-arp
- show arp
- show hosts
- show ip interface

1.1.1 arp

Syntax

To configure static ARP mapping, run the following command.

arp *ip-address hardware-address* **vlan** *vlan-id* [**alias**]

To return to the default setting, use the no form of this command.

no arp *ip-address* **vlan** *vlan-id*

Parameters

Parameters	Description
ip-address	IP address corresponding to the local data-link address.
hardware-address	Physical address of local data-link address

vlan-id	The vlan interface belongs to the static arp
alias	(optional) OLT responds to ARP requests as if it were the interface of the specified address.

Default Value

No entries are permanently installed in the ARP cache.

Command Mode

Global configuration mode

Usage Guidelines

The common host all supports dynamic ARP analysis, so user doesn’t need to configure static ARP entries for host.

Usually to delete static arp, run no arp *ip_address vlan*. If the vlan interface belongs to a static arp is deleted, delete the static arp by running no arp *ip_address*.

Example

The following example shows that the MAC address of the host with IP address 1.1.1.1 is set to 00:12:34:56:78:90.

```
Switch_config# arp 1.1.1.1 00:12:34:56:78:90 vlan 1
```

Related Command

clear arp-cache

1.1.2 arp pending-time

Syntax

To set the waiting time of ARP cache resolution, run the following command.

arp pending-time *seconds*

To return to the default setting, use the no form of this command.

no arp pending-time

Parameters

Parameters	Description

seconds	Sets the waiting time of ARP cache resolution, whose unit is second. The value ranges from 2 to 15.

Default Value

15 seconds

Command Mode

Global configuration mode

Usage Guidelines

The first ARP cache resolution will generate an incomplete entry and this command will then be used to set the life-time of this incomplete entry.

Example

The following example shows how to set the waiting time of ARP cache resolution to 10 seconds.

```
Switch_config# arp pending-time 10
```

Related Command

show arp

1.1.3 arp max-incomplete

Syntax

To set the maximum number of incomplete ARP entries, run the following command.

arp max-incomplete *number*

To return to the default setting, use the no form of this command.

no arp max-incomplete

Parameters

Parameters	Description
number	Sets the maximum number of incomplete ARP entries. The value ranges from 0 to 1024.

Default Value

The default value is 0, meaning no threshold exists.

Command Mode

Global configuration mode

Usage Guidelines

This command can be used to set the maximum number of the incomplete entries during ARP cache resolution.

Example

The following example shows how to set the maximum number of the incomplete ARP cache entries to 10:

```
Switch_config# arp max-incomplete 10
```

Related Command

show arp

1.1.4 arp max-gw-retries

Syntax

To set the maximum retransmissions of the Re-Detect packets, run the following command.

arp max-gw-retries *number*

To return to the default setting, use the no form of this command.

no arp max-gw-retries

Parameters

Parameters	Description
number	Sets the maximum retransmissions of the Re-Detect packets. The value ranges from 0 to 5.

Default Value

3

Command Mode

Global configuration mode

Usage Guidelines

The ARP entries, which the routing entry gateway depends on, require being redetected at their aging so that the promptness and correctness of the hardware subnet routing can be guaranteed. This command is here used for setting the maximum ARP retransmissions in the redetection process. The bigger its value is, the greater chance the detection has.

Example

The following example shows how to set the maximum retransmissions of the Re-Detect packets to 5:

```
Switch_config# arp max-gw-retries 5
```

Related Command

show arp

1.1.5 arp retry-allarp

Syntax

To set re-detection when ARP entry is aging, run the following command.

arp retry-allarp

To return to the default setting, use the no form of this command.

no arp retry-allarp

Parameters

None

Command Mode

Global configuration mode

Usage Guidelines

By default, redetection is conducted only to the aging ARPs, which the routing entry gateway depends on. However, if this command is enabled, redetection will be conducted towards all types of aging ARP entries.

Example

The following example shows how to enable redetection to be carried out to all aging ARP entries.

```
Switch_config# arp retry-allarp
```

Related Command

show arp

1.1.6 arp timeout

Syntax

To configure the exist time that a dynamic ARP entry remains in the Address Resolution Protocol (ARP) cache, use the arp timeout.

arp timeout *seconds*

To configure the exist time that a dynamic ARP entry remains in the Address Resolution Protocol (ARP) cache, use the arp timeout.

no arp timeout

default arp timeout

Parameters

Parameters	Description
seconds	Time in seconds that an entry remains in the ARP cache. A value of zero means that entries are never cleared from the cache. The value ranges from 0 to 4294967.

Default Value

14400 seconds (4 hours)

Command Mode

VLAN interface configuration mode

Usage Guidelines

This command is ignored when it is not configured on interfaces using ARP. The show interface command displays the ARP timeout value, as seen in the following example from the show interfaces command:

ARP type: ARPA, ARP timeout 04:00:00

Example

The following example sets the ARP timeout to 900 seconds on interface vlan 10 to allow entries to time out more quickly than the default.

Switch_config# **interface vlan** *10*

Switch_config_v10# **arp timeout** *900*

Related Command

show interface

1.1.7 arp dynamic

Syntax

To enable the dynamic arp learning of vlan interface, run the following command. To return to the default setting, use the no form of this command.

arp dynamic

[no] arp dynamic

Parameters

None

Default Value

The dynamic arp learning of vlan interface is enabled.

Command Mode

VLAN interface configuration mode

Usage Guidelines

The command allows the dynamic arp learning of vlan interface by default.

Example

The following example shows how to disable the dynamic arp learning of the vlan interface on vlan 10.

Switch_config# interface vlan *10*

Switch_config_v10# no arp dynamic

Related Command

None

1.1.8 arp send-gratuitous

Syntax

To configure ARP send-gratuitous function, use the arp send-gratuitous command.

arp send-gratuitous [**interval** *value*]

To disable ARP send-gratuitous function, use no arp send-gratuitous command.

no arp send-gratuitous

Parameters

Parameters	Description
interval	Sets the intervals of arp send-gratuitous
value	Sets the time interval; the default is 120 seconds. The range is 15 to 600 seconds

Default Value

120s

Command Mode

VLAN interface configuration mode

Example

The following example start arp send-gratuitous on Interface Vlan 1, and set the send interval as 3 minutes.

```
Switch_config# interface vlan 1
switch_config_v1# arp send-gratuitous interval 180
```

Related Command

arp

1.1.9 clear arp-cache

Syntax

To clear all dynamic entries from the ARP cache, use the clear arp-cache command.

clear arp-cache [*ip-address* [*mask* **|** **vlan** *vlanid*]]

Parameters

Parameters	Description
ip-address	IP or subnets
mask	Subnet mask
vlanid	vlan ID

Default Value

None

Command Mode

EXEC mode

Example

The following example shows how to clear all dynamic ARP cache.

```
Switch_config# clear arp-cache
```

Related Command

arp

1.1.10 ip address

Syntax

To set an IP address and mask for an interface, use the ip address command. Currently, there is no strict regulation to distinguish A.B.C IP address. But multicast address and broadcast address cannot be used (all host section is ‘1’). Other than the Ethernet, multiple interfaces of other types can be connected to the same network. Other than the unnumbered interface, the configured network range of the Ethernet interface cannot be the same as the arbitrary interfaces of other types. Usually one interface usually can configure one master address and numerous secondary addresses. You should configure the primary address before configuring the secondary address. IP packets generated by the system, if the upper application does not specify the source address, the OLT will use the IP address configured on the sending interface that on the same network range with the gateway as the source address of the packet. If the IP address is uncertain (like interface route), the OLT will use the primary address of the sending interface. If the ip address is not configured on an interface, also it is not the unnumbered interface, and then this interface will not deal with any IP packet.

ip address *ip-address mask* [**secondary**]

To clear an or all IP addresses on the interface, run the following command.

no ip address *ip-address mask*

no ip address

Parameters

Parameters	Description
ip-address	IP address
mask	Mask of the IP network
secondary	(optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

Default Value

No IP address is defined for the interface.

Command Mode

VLAN interface configuration mode, monitoring mode

Usage Guidelines

If any OLT on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet.

When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.

Example

In the following example, 202.0.0.1 is the primary address, 255.255.255.0 is the mask and 203.0.0.1 and 204.0.0.1 are secondary addresses for Ethernet VLAN 10.

```
Switch_config# interface vlan 10
Switch_config_v10# ip address 202.0.0.1 255.255.255.0
Switch_config_v10# ip address 203.0.0.1 255.255.255.0 secondary
```

Switch_config_v10# **ip address** *204.0.0.1 255.255.255.0* **secondary**

1.1.11 ip directed-broadcast

Syntax

To enable the translation of a directed broadcast to physical broadcasts, run ip directed-broadcast [access-list-namer].

ip directed-broadcast [*access-list-namer*]

To return to the default setting, use the no form of this command.

no ip directed-broadcast

Parameters

Parameters	Description
access-list-name	(Optional) Access list name. If specified, a broadcast must pass the access list to be forwarded.

Default Value

By default, all IP directed broadcasts are dropped.

Command Mode

Interface configuration mode

Example

The following example enables forwarding of IP directed broadcasts on Ethernet interface vlan 10:

```
Switch_config# interface vlan 10
Switch_config_v10# ip directed-broadcast
```

1.1.12 ip forward-protocol

Syntax

To designate to forward which UDP protocol wire broadcasting packet, run the following command.

ip forward-protocol udp [*port*]

To designate to forward the default UDP protocol wire broadcasting packet, run the following command.

no ip forward-protocol udp [*port*]

default ip forward-protocol udp

Parameters

Parameters	Description
Port	(optional) Destination port that controls which UDP requests are forwarded. The value ranges from 0 to 65535.

Default Value

The netbios name service request is forwarded by default.

Command Mode

Global configuration mode

Usage Guidelines

The netbios name service request is forwarded by default. Not to forward netbios name service request, use one of the following commands:

no ip forward-protocol udp netbios-ns

no ip forward-protocol udp 137

The following command is used to disable forwarding all UDP broadcasting requests.

no ip forward-protocol udp

Example

```
switch_config# ip forward-protocol udp 137
```

Related Command

ip helper-address

1.1.13 ip helper-address

Syntax

To forward IP directional broadcast packet to designated IP helper address, run the following command.

ip helper-address *address*

To return to the default setting, use the no form of this command.

no ip helper-address *address*

Parameters

Parameters	Description
address	IP helper address

Default Value

Non-configured IP helper address

Command Mode

VLAN interface configuration mode

Usage Guidelines

The ip helper-address command does not work on an X.25 interface on a destination OLT because the OLT cannot determine if the packet was intended as a physical broadcast.

Example

The following example configures IP helper-address 1.0.0.1 on the interface vlan 10.

```
Switch_config# interface vlan 10
Switch_config_v10# ip helper-address 1.0.0.1
```

Related Command

ip forward-protocol udp

1.1.14 ip host

Syntax

To define the name-address mapping of the static host, run ip host name hostname address.

ip host *name address*

To return to the default setting, use the no form of this command.

no ip host *name*

Parameters

Parameters	Description
name	Name of the host

Address	IP Address

Default Value

No mapping is configured.

Command Mode

Global configuration mode

Usage Guidelines

None

Example

The following example shows how to set the name of the host with IP address 202.96.1.3 to dns-server.

Switch_config# **ip host** *dns-server 202.96.1.3*

1.1.15 ip proxy-arp

Syntax

To enable proxy Address Resolution Protocol (ARP) on an interface, use the ip proxy-arp command.

ip proxy-arp [same-interface]

To disable proxy Address Resolution Protocol (ARP) on an interface, run the following command.

no ip proxy-arp [same-interface]

Parameters

Parameters	Description
same-interface	Enables proxy ARP on the same interface.

Default Value

Enables proxy ARP. Forbid proxy ARP on the same interface.

Command Mode

VLAN interface configuration mode

Usage Guidelines

When routing OLT receives ARP requirements, if routing OLT has the routing path to required IP address, and the routing interface and the interface receive the requirements are different, routing OLT will send ARP reaction from its own MAC address, and then it forward actual data packets when receive them. In this case, even if one host does not know the network topology, or without configured accurate routing, it can also communicate with remote terminal. The remote host is connected with the routing OLT in the same physical subnet.

If the host need routing OLT to provide such function, then the host and the routing OLT must be in the same IP network, or its IP address is regarded in the IP subnet of routing OLT, or rather, they can use different masks, or routing OLT cannot provide such service.

Example

The following example enables the proxy ARP function on the interface VLAN 10.

```
Switch_config# interface vlan 10
Switch_config# ip proxy-arp
```

1.1.16 show arp

Syntax

To display the entries in the Address Resolution Protocol (ARP) table, including the ARP mapping of interface IP address, the static ARP mapping that user configures and the dynamic ARP mapping, run the following command.

show arp [**local | incomplete | temporary|** {*address* [*netmask* | *vlan-id*]}]

Parameters

Parameters	Description
local	Stands for the local port arp
incomplete	Stands for the incomplete arp
temporary	temporary arp
address	IP address
netmask	netmask, It is used for showing all arp in the network section.
vlan-id	vlan port belongs to arp

Default Value

None

Command Mode

Other modes except the user mode

Usage Guidelines

Shown information include:

Protocol	Protocol, the type of physical address mapping, for instance, IP.
Address	Address, the network address mapping the physical address, for instance, IP address.
Age	Time to Live, from generating ARP entries to now. Unit: min. The value will not be affected if the OLT uses the ARP entry.
Hardware Address	physical address, the address corresponding to the network address. The entry has not resolved is empty.
Type	Type, means the encapsulation type the interface uses, such as ARPA and SNAP.
Interface	Interface, the interface connects to the network address.

Example

The following example shows ARP cache:

```
switch# show arp
Protocol   IP Address        Age(min)  Hardware Address    Type   Interface
   IP      192.168.20.77         11    00:30:80:d5:37:e0   ARPA   vlan 10
   IP      192.168.20.33          0       Incomplete
   IP      192.168.20.22          -    08:00:3e:33:33:8a   ARPA   vlan 10
   IP      192.168.20.124         0    00:a0:24:9e:53:36   ARPA   vlan 10
   IP      192.168.0.22           -    08:00:3e:33:33:8b   ARPA   vlan 11
```

The following example shows the detailed information of specific arp entry:

```
Switch# show arp 90.0.0.3 vLAN 1
ARP entry with IP 90.0.0.3
Protocol Address:     90.0.0.3
Age(in minutes):      0
Hardware Address:       a0:b3:cc:fe:87:c6
Type:                   ARPA [U]flgs 0x1
Interface:            v1(g0/1)
```

1.1.17 show hosts

Syntax

To show all entries in host name-address cache, run this command.

show hosts

Parameters

The command has no parameters or keywords.

Default Value

None

Command Mode

Other modes except the user mode

Usage Guidelines

None

Example

The command shows all host name/address mapping:

```
Switch_config# show hosts
```

1.1.18 show ip interface

Syntax

To show IP configuration of the interface, run this command.

show ip interface [**type** *number* **|** ***brief***]

Parameters

Parameters	Description
type	(Optional) interface type
number	(Optional) interface number
brief	(Optional) Shows ip protocol brief of all vlan interfaces.

Command Mode

Other modes except the user mode

Usage Guidelines

If the link layer of an interface can effectively transmit and receive the data, the interface is available, whose state is Protocol Up. If an IP address is configured on the interface, the OLT will add an direct-through route to the routing table. If the link-layer protocol is disabled, that is, if the link-layer protocol is Protocol Down, the direct-through route will be deleted. If the interface type and the number of the interface is specified, only the information about the specified interface is displayed. Otherwise, the information about the IP configuration of all interfaces is displayed.

Example

The following example shows the IP configuration of interface VLAN 11.

```
switch#show ip interface vlan 10
VLAN1 is up, line protocol is up
  Internet address is 10.112.4.160/24
  Broadcast address is 10.112.4.255
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.9 224.0.0.6 224.0.0.5
                                    224.0.0.2 224.0.0.1
  Outgoing access list is not set
  Inbound  access list is not set
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
```

Description

Domain	Description
vlan 11 is up	If the interface hardware is usable, the interface is marked "up." For an interface to be usable, both the interface hardware and line protocol must be up.
line protocol is up	If the interface can provide two-way communication, the line protocol is marked "up." For an interface to be usable, both the interface hardware and line protocol must be up.
IP address	IP address and mask for interface
Broadcast address	Displays broadcast address
MTU	Displays the MTU value set on the interface.
Helper address	Displays helper address
Directed broadcast	Forwards the directed broadcast packets.

forwarding	
Multicast reserved groups joined	Multicast groups added to the interface
Outgoing ACL	Outgoing access control list used by the interface
Incoming ACL	Incoming access control list used by the interface
IP fast switching	Enables fast switching on the interface by the OLT.
Proxy ARP	Enables the proxy ARP on the interface.
ICMP redirects	Forwards the ICMP redirect packet on the interface.
ICMP unreachables	Forwards the ICMP-unreachable packet on the interface.
ICMP mask replies	Forwards the ICMP-mask-replies packet on the interface.

Chapter 2 DHCP Client Configuration Commands

2.1 DHCP Client Configuration Commands

DHCP Client Configuration Commands include:

- ip address dhcp
- ip dhcp client
- ip dhcp-server
- show dhcp lease
- show dhcp server
- debug dhcp

The chapter describes the DHCP configuration commands. These commands are used to configure and monitor the DHCP running on the OLT.

2.1.1 ip address dhcp

Syntax

To obtain an IP address for the interface by Dynamic Host Configuration Protocol (DHCP).

ip address dhcp

To return to the default setting, use the no form of this command.

no ip address dhcp

Parameters

None

Default Value

None

Command Mode

VLAN interface configuration mode

Usage Guidelines

The **ip address dhcp** command allows an interface to obtain an IP address through DHCP, which is very useful to dynamically connecting ISP through the Ethernet interface.

When the dynamic IP address is obtained and the ip address dhcp command is configured, the OLT sends the DHCPDISCOVER message to the DHCP server in the network.

When **no ip address dhcp** is configured, the OLT sends the DHCPRELEASE message.

Example

The following example shows that theVLAN11 interface obtains the IP address through the DHCP protocol.

```
Switch_config# interface vlan 11
Switch_config_v11# ip address dhcp
```

Related Command

ip dhcp client

ip dhcp-server

show dhcp lease

show dhcp server

2.1.2 ip dhcp client

Syntax

To configure the parameters of the local OLT DHCP client, run the following command:

ip dhcp client { **minlease** *seconds* **|** **retransmit** *count* **|** **select** *seconds* }**| class_identifier** *WORD* **| client_identifier | retry_interval** <*1-1440*> **| timeout_shut | bootfileaddmac | tftpdownload}**

To configure the parameters of the local OLT DHCP client as the default value, run the following command:

no ip dhcp client { **minlease | retransmit | select | class_identifier | client_identifier | retry_interval | timeout_shut | bootfileaddmac | tftpdownload** }

Parameters

Parameters	Description
minlease *seconds*	(Optional) Stands for the acceptable minimum lease time, which ranges from 60 to 86400 seconds and an optional parameter.

retransmit *count*	(Optional) Stands for the retransmission times of the protocol packets, which ranges from 1 to 10 and is an optional parameter.
select *seconds*	(Optional) Stands for the interval of SELECT, which ranges from 5 to 30 and is an optional parameter.
class_identifier *WORD*	(Optional) Sets the class ID belongs to the client
client_identifier hrd_ether	(Optional) Sets the type of client ID to Ethernet
retry_interval *<1-1440>*	(Optional) Sets retry interval
timeout_shut	(Optional) Timeout to shutdown the interface
bootfileaddmac	(optional) Enable DHCP file name to add MAC address of the client
tftpdownload	(Optional) Enable TFTP download function

Default Value

The Default value of minlease parameter is 60 seconds.

The default value of the retransmit parameter is 4 times.

The default value of the select parameter is 5 seconds.

class_identifier no parameter default value

client_identifier the parameter default value is the character string

retry_interval the default value is 1 minute

timeout_shut no parameter default value

bootfileaddmac no parameter default value

tftpdownload no parameter default value

Command Mode

Global configuration mode

Usage Guidelines

You can adjust these parameters according the requirements of the network structure and the DHCP server.

If the negative forms of these commands are set, these parameter will resume their default values.

Example

The following example shows how to set on the DHCP client of OLT the acceptable minimum lease time to 100 seconds:

```
Switch_config# ip dhcp client minlease 100
```

The following example shows how to set the retransmission times of the protocol packets on the DHCP client of OLT to 3:

```
Switch_config# ip dhcp client retransmit 3
```

The following example shows, on the DHCP client of OLT, how to set the interval of SELECT to 10 seconds:

```
Switch_config# ip dhcp client select 10
```

Related Command

ip address dhcp

ip dhcp-server

show dhcp lease

show dhcp server

2.1.3 ip dhcp-server

Syntax

To designate the known DHCP server address, run the following command.

ip dhcp-server *ip-address*

To return to the default setting, use the no form of this command.

no ip dhcp-server *ip-address*

Parameters

Parameters	Description
ip-address	IP address of the DHCP server

Default Value

There is no default IP address of the DHCP server.

Command Mode

Global configuration mode

Usage Guidelines

You can designate an IP address for a DHCP server by using this command, which will not replace the previously designated IP address of the DHCP server.

But the previously designated IP address of the DHCP server can be removed by the negative form of this command.

Example

The following example shows how to specify on OLT a server, whose IP address is 192.168.20.1, to be the DHCP server:

```
Switch_config# ip dhcp-server 192.168.20.1
```

Related Command

ip address dhcp

ip dhcp client

show dhcp lease

show dhcp server

2.1.4 show dhcp lease

Syntax

To browse the distribution information of the DHCP server of the current OLT, run the following command.

show dhcp lease

Parameters

None

Default Value

None

Command Mode

Other modes except the user mode

Usage Guidelines

You can use this command to browse the distribution information of the DHCP server of the current OLT.

Example

The following example shows how to display the DHCP distribution information of OLT:

```
switch# show dhcp lease
Temp IP addr: 192.168.20.3    for peer on Interface: vlan11
Temp    sub net mask: 255.255.255.0
   DHCP Lease server: 192.168.1.3, state: 4 Rebinding
   DHCP transaction id: 2049
   Lease: 86400 secs,    Renewal: 43200 secs,    Rebind: 75600 secs
Temp default-gateway addr: 192.168.1.2
   Next timer fires after: 02:34:26
   Retry count: 1      Client-ID: router-0030.80bb.e4c0-v11
```

Related Command

ip address dhcp
ip dhcp client
ip dhcp-server
show dhcp server
debug dhcp

2.1.5 show dhcp server

Syntax

To designate the known DHCP server information, run the following command.

show dhcp server

Parameters

None

Default Value

None

Command Mode

Other modes except the user mode

Usage Guidelines

This command is used to display the known information of the DHCP server.

Example

The following example shows how to display the already known information about the DHCP server.

```
switch# show dhcp sever
DHCP server: 255.255.255.255
  Leases:   0
  Discovers: 62 Requests: 0       Declines: 0       Releases: 0
  Offers:     0   Acks:       0       Naks:       0       Bad:        0
  Subnet: 0.0.0.0,         Domain name:
```

Related Command

ip address dhcp

ip dhcp client

ip dhcp-server

show dhcp lease

2.1.6 debug dhcp

Syntax

To enable dhcp protocol process information output, run the following command.

debug dhcp [**detail**]

To return to the default setting, use the no form of this command.

no debug dhcp [**detail**]

Parameters

Parameters	Description
detail	Means to display the content of the DHCP packet.

Default Value

Relative information is not shown.

Command Mode

Privileged mode

Usage Guidelines

The following example shows some key information about DHCP processing:

```
switch# debug dhcp
```

Related Command

show dhcp lease

Chapter 3 DHCP Server Configuration Commands

3.1 DHCPD Configuration Commands

DHCPD configuration commands include:

- ip dhcpd ping packet
- ip dhcpd ping timeout
- ip dhcpd write-time
- ip dhcpd database-agent
- ip dhcpd database-file
- ip dhcpd database-realtime
- ip dhcpd relay-STB
- ip dhcpd sname-option
- ip dhcpd server-name
- ip dhcpd bootp
- ip dhcpd bootfile-name
- ip dhcpd bootfile-option
- ip dhcpd abandon-time
- ip dhcpd snooping arp
- ip dhcpd pool
- ip dhcpd enable

3.1.1 ip dhcpd ping packets

Syntax

To set the number of ICMP packet transmitting when it is checking whether the address is distributed, run the following command.

ip dhcpd ping packets *pkgs*

To return to the default setting, use the no form of this command.

no ip dhcpd ping packets *pkgs*

Parameters

Parameters	Description
pkgs	<0-10> Number of ping packets when they detect the address conflicts

Default Value

2

Command Mode

Global configuration mode

Usage Guidelines

The command is used to configure n ICMP packets when the DHCP server is checking whether the address is distributed.

ip dhcpd ping packets *n*

Example

The following example shows that the DHCP server transmits one ICMP packet when it is checking whether the address is distributed.

```
Switch_config# ip dhcpd ping packets 1
```

3.1.2 ip dhcpd ping timeout

Syntax

The following example shows how to set the timeout time of waiting for the response of ICMP packets when the DHCP server is checking whether the address is distributed.

ip dhcpd ping timeout *timeout*

To return to the default setting, use the no form of this command.

no ip dhcpd ping timeout *timeout*

Parameters

Parameters	Description
timeout	Stands for the timeout time of waiting for the response of the ICMP packet when the DHCP server checks address distribution

	(Unit: 100ms). The value ranges from 0 to 20.

Default Value

5

Command Mode

Global configuration mode

Usage Guidelines

This command is used to set to n*100ms the timeout time of waiting for the response of ICMP packets when the DHCP server is checking whether the address is distributed.

ip dhcpd ping timeout *n* .

Example

The following example shows how to set to 300ms the timeout time of waiting for the response of ICMP packets when the DHCP server is checking whether the address is distributed.

```
Switch_config# ip dhcpd ping timeout 3
```

3.1.3 ip dhcpd write-time

Syntax

To set the time interval of DHCP server writing the address distribution information into the database, run the following command.

ip dhcpd write-time *time*

To return to the default setting, use the no form of this command.

no ip dhcpd write-time

Parameters

Parameters	Description
time	<0-43200>mins, the period of backup binding table

Default Value

0 means disabled

Command Mode

Global configuration mode

Usage Guidelines

The following command is used to make the DHCP server write the address distribution information to the database every n minutes.

ip dhcpd write-time n

It is recommended the ip dhcpd write-time is smaller than the default value.

Example

The following example shows that the DHCP server writes the address distribution information to the database every other day.

Switch_config# **ip dhcpd write-time** *1440*

3.1.4 ip dhcpd database-agent

Syntax

To set the PC address for saving the address distribution information of the DHCP server, run the following command.

ip dhcpd database-agent *ip-address*

To return to the default setting, use the no form of this command.

no ip dhcpd database-agent *ip-address*

Parameters

Parameters	Description
Ip-address	Stands for the address of the PC, to which the DHCP server will save the address distribution information in the file format.

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

You can use the following command to set the address of PC on which the DHCP server saves the address distribution information:

ip dhcpd database-agent *X. X. X. X*

If this address is not set, the address distribution information will be saved to the flash.

Note: Before the address distribution information is saved, PC should enable the TFTP server and also PC and the DHCP server should connect correctly.

Example

Switch_config# **ip dhcpd database-agent** *192.168.1.1*

3.1.5 ip dhcpd database-file

Syntax

To save the address distribution file name of the DHCP server, run the following command.

ip dhcpd database-file *word* [time-stamp]

To return to the default setting, use the no form of this command.

no ip dhcpd database-file

Parameters

Parameters	Description
word	Stands for the address of the PC, to which the DHCP server will save the address distribution information in the file format.
time-stamp	file name addition time stamp

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

You can use the following command to set the address of PC on which the DHCP server saves the address distribution information. The file name is *word*.

ip dhcpd database-agent X. X. X. X

ip dhcpd database-file *word*

If this address is not set, the address distribution information will be saved to the flash.

Note: Before the address distribution information is saved, PC should enable the TFTP server and also PC and the DHCP server should connect correctly.

Example

```
Switch_config# ip dhcpd database-agent 192.168.1.1
Switch_config# ip dhcpd database-file dbfile time-stamp
```

3.1.6 ip dhcpd database-realtime

Syntax

To save the change of cache entry in time to the data base file, run the following command.

ip dhcpd database-realtime

To return to the default setting, use the no form of this command.

no ip dhcpd database-realtime

Parameters

None

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command is used to save the change of cache entry in time to the data base file.

Example

```
Switch_config# ip dhcpd database-realtime
```

3.1.7 ip dhcpd relay_STB

Syntax

To forward STB DHCP data packet, run the following command.

ip dhcpd relay_STB

To return to the default setting, use the no form of this command.

no ip dhcpd relay_STB

Parameters

None

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command is used to forward STB DHCP data packet.

Example

```
Switch_config# ip dhcpd relay-STB
```

3.1.8 ip dhcpd sname-option

Syntax

To enable DHCP TFTP server name option, run the following command.

ip dhcpd sname-option

To return to the default setting, use the no form of this command.

no ip dhcpd sname-option

Parameters

None

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command is used to enable DHCP TFTP server name option.

Example

```
Switch_config# ip dhcpd sname-option
```

3.1.9 ip dhcpd server-name

Syntax

To configure DHCP optional server host name, run the following command.

ip dhcpd server-name *word*

To return to the default setting, use the no form of this command.

no ip dhcpd server-name

Parameters

Parameters	Description
word	optional server host name

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The following command is used to configure DHCP optional server host name.

Example

```
Switch_config# ip dhcpd server-name 192.168.0.1
```

3.1.10 ip dhcpd bootp

Syntax

To configure DHCP supporting BOOTP client, run the following command.

ip dhcpd bootp [auto-bind]

To return to the default setting, use the no form of this command.

no ip dhcpd bootp

Parameters

Parameters	Description
auto-bind	Allows BOOTP client distributing auto binding address.

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command is used to configure DHCP supporting BOOTP client.

Example

```
Switch_config# ip dhcpd bootp
```

3.1.11 ip dhcpd bootfile-name

Syntax

To configure DHCP file domain, run the following command.

ip dhcpd bootfile-name *word*

To return to the default setting, use the no form of this command.

no ip dhcpd bootfile-name

Parameters

Parameters	Description
word	File Name

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command is used to configure DHCP file domain.

Example

```
Switch_config# ip dhcpd bootfile-name btfile
```

3.1.12 ip dhcpd bootfile-option

Syntax

To configure DHCP enabling file name option, run the following command.

ip **dhcpd bootfile-option**

To return to the default setting, use the no form of this command.

no **ip dhcpd bootfile-option**

Parameters

None

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command is used to configure DHCP enabling file name option.

Example

```
Switch_config# ip dhcpd bootfile-option
```

3.1.13 ip dhcpd abandon-time

Syntax

To configure the time interval of clearing one "abandoned" mark, run the following command.

ip dhcpd abandon-time *time*

To return to the default setting, use the no form of this command.

no ip dhcpd abandon-time

Parameters

Parameters	Description
time	The time of DHCP server clearing the abandon mark. Value Range: 1-8640 (unit: hour)

Default Value

2 hours

Command Mode

Global configuration mode

Usage Guidelines

To set the interval of clearing the “Abandoned” mark, run the following command in global mode: (When the dhcp server is distributing address, the address will be labeled with abandon mark if the address is founded to have been used already. The address will not be detected until it is cleared.)

Example

The following example shows how to set the time interval of clearing the abandon mark to 10 hours.

Switch_config# **ip dhcpd abandon-time** *10*

3.1.14 ip dhcpd snooping arp

Syntax

To enable ARP mapping protection, run the following command. To return to the default setting, use the no form of this command.

ip dhcpd snooping arp

[no] ip dhcpd snooping arp

Parameters

None

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command can be used to enable the ARP map protection. When this command is set, the DHCP server will establish an ARP map between the MAC address and distributed IP address of the DHCP client, and then protect this ARP map.

Example

```
Switch_config# ip dhcpd snooping arp
```

3.1.15 ip dhcpd pool

Syntax

To add DHCP address pool, run the following command.

ip dhcpd pool *name*

To reduce DHCP address pool, run the following command.

no ip dhcpd pool *name*

Parameters

Parameters	Description
name	Stands for the name of the DHCP address pool.

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

You can use the following command to add a DHCP address pool, whose name is name, and to enter the DHCP address pool configuration mode.

ip dhcpd pool *name*

Example

The following example shows how to add the DHCP address pool named test and enter the DHCP address pool configuration mode:

```
Switch_config# ip dhcpd pool test
```

3.1.16 ip dhcpd enable

Syntax

To enable DHCP service, run the following command. To return to the default setting, use the no form of this command.

ip dhcpd enable

[no] ip dhcpd enable

Parameters

None

Default Value

The DHCP service is disabled by default.

Command Mode

Global configuration mode

Usage Guidelines

The command is used to enable the DHCP service. In this instance, the DHCP server also supports the relay operation, and as to those address requests that the DHCP server cannot distribute, its interface, on which the ip helper-address command is set, will forward the DHCP requests.

Example

The following example shows how to enable the DHCP service.

```
Switch_config# ip dhcpd enable
```

3.1.17 ip dhcpd sname-bootfile-option-force

Syntax

To compulsorily enable DHCP TFTP server name option (option:66) and DHCP enabling file name option (option: 67).

ip dhcpd sname-bootfile-option-force

To return to the default setting, use the no form of this command.

no ip dhcpd sname-bootfile-option-force

Parameters

None

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command is used to compulsorily enable DHCP TFTP server name option (option:66) and DHCP enabling file name option (option: 67).

Example

```
Switch_config# ip dhcpd sname-bootfile-option-force
```

3.2 DHCPD Address Pool Configuration Commands

DHCPD Address Pool Configuration Commands

- network
- range
- default-router
- dns-server
- domain-name
- lease
- netbios-name-server
- ip-bind

3.2.1 network

Syntax

To configure the network address of DHCP address pool, run the following command.

network *ip-addr netmask*

To return to the default setting, use the no form of this command.

no network *ip-addr*

Parameters

Parameters	Description
ip-addr	Stands for the network address of an address pool, which is used for automatic distribution.

netmask	Subnet mask

Default Value

None

Command Mode

DHCP address pool configuration mode

Usage Guidelines

This command is used to set the network address of the address pool of automatic distribution. This command is used only in automatic distribution mode.

When this command is set, you must make sure that the network ID in an IP address of a port, on which the DHCP packets are received, is same as the network.

Example

The following example shows how to set the network address of the DHCP address pool to 192.168.20.0 and its subnet mask to 255.255.255.0.

```
Switch_config# ip dhcpd pool test
Switch_config_dhcp# network 192.168.20.0 255.255.255.0
```

3.2.2 range

Syntax

To set the address range of automatic distribution, run the following command.

range *low-addr high-addr*

To return to the default setting, use the no form of this command.

no range *low-addr high-addr*

Parameters

Parameters	Description
low-addr	Stands for the start address of the automatic address distribution area.
high-addr	Stands for the end address of the automatic address distribution area.

Default Value

None

Command Mode

DHCP address pool configuration mode

Usage Guidelines

This command is to set the address range of automatic distribution. Each address pool can be divided into 8 ranges at the maximum, and each range must be in the network. This command is used only in automatic distribution mode.

Example

The following example shows how to set the address distribution area of the DHCP address pool to be from 192.168.20.210 to -192.168.20.219.

Switch_config# **ip dhcpd pool** *test*

Switch_config_dhcp# **range** *192.168.20.210 192.168.20.219*

3.2.3 default-router

Syntax

To set the default route that is distributed to the client, run the following command.

default-router {*ip-addr*}&<1-4>

To return to the default setting, use the no form of this command.

no default-router

Parameters

Parameters	Description
ip-addr	Sets the default route that is distributed to the client.

Default Value

None

Command Mode

DHCP address pool configuration mode

Usage Guidelines

The command can be used to set the default route that is distributed to the client. Up to 4 default routes can be configured, which are separated by the space.

Example

The following example shows how to set the default route, which will be distributed to the DHCP client, to 192.168.20.1.

Switch_config# **ip dhcpd pool** *test*

Switch_config_dhcp# **default-router** *192.168.20.1*

3.2.4 dns-server

Syntax

To configure the address of DNS server, which is distributed to the client, run the following command.

dns-server {*ip-addr*}&<1-4>

To return to the default setting, use the no form of this command.

no dns-server

Parameters

Parameters	Description
ip-addr	Sets the address of the DNS server, which is distributed to the client.

Default Value

None

Command Mode

DHCP address pool configuration mode

Usage Guidelines

The command is used to set the address of the DNS server that is distributed to the client. Up to 4 DNS servers can be configured, which are separated by the space.

Example

The following example shows how to set the address of DNS server, which is distributed to the client, to 192.168.1.3.

Switch_config# **ip dhcpd pool** *test*

Switch_config_dhcp# **dns-server** *192.168.1.3*

3.2.5 domain-name

Syntax

To configure a domain name, which is distributed to the client, run the following command.

domain-name *name*

To return to the default setting, use the no form of this command.

no domain-name

Parameters

Parameters	Description
name	Stands for the domain name which is distributed to the client.

Default Value

None

Command Mode

DHCP address pool configuration mode

Usage Guidelines

This command is used to set a domain name, which is distributed to the client.

Example

The following example shows how to set the domain name, which is distributed to the client, to test.domain.

Switch_config# **ip dhcpd pool** *test*

Switch_config_dhcp# **domain-name** *test.domain*

3.2.6 lease

Syntax

To set the time limitation of the address, which is distributed to the client, run the following command.

lease {*days* [*hours*] [*minutes*] **| infinite}**

To return to the default setting, use the no form of this command.

no lease

Parameters

Parameters	Description
days	Stands for the days of address distribution.
hours	Stands for the hours of address distribution.
minutes	Stands for the minutes of address distribution.
infinite	Means that the addresses will be distributed forever.

Default Value

One day

Command Mode

DHCP address pool configuration mode

Usage Guidelines

This command is used to set the time limitation of the address, which is distributed to the client.

Example

The following example shows how to set the time limitation of address distribution to 2 days and 12 hours.

```
Switch_config# ip dhcpd pool test
Switch_config_dhcp# lease 2 12
```

3.2.7 netbios-name-server

Syntax

To set the address of the netbios name server, which is distributed to the client.

netbios-name-server {*ip-addr*}&<1-4>

To return to the default setting, use the no form of this command.

no netbios-name-server

Parameters

Parameters	Description
ip-addr	Sets the address of the netbios name server, which is distributed to the client.

Default Value

None

Command Mode

DHCP address pool configuration mode

Usage Guidelines

The command is used to set the address of the Netbios name server that is distributed to the client. Up to 4 Netbios name servers can be configured, which are separated by the space.

Example

The following example shows how to set the address of the netbios name server to 192.168.1.10.

```
Switch_config# ip dhcpd pool test
Switch_config_dhcp# netbios-name-server 192.168.1.10
```

3.2.8 ip-bind

Syntax

To set the host's address of the address pool of automatic distribution, run the following command.

ip-bind *ip-addr* **{hardware-address** *WORD* [*type*] **| host-name** *WORD* **| identifier** *WORD*}

To return to the default setting, use the no form of this command.

no ip-bind *ip-addr*

Parameters

Parameters	Description
hardware-address *WORD [type]*	WORD is used to match the hardware address of the client. type is used to match the network type of the user.
host-name *WORD*	It is used to match the user host name.
Identifier *WORD*	It is used to match the client ID.

Default Value

None

Command Mode

DHCP address pool configuration mode

Usage Guidelines

This command is used to set the address of the host whose address pool is used for manual distribution.

Example

The following example shows how to set the hardware address of DHCP manual distributing address 1.1.1.1 to 10-a0-0c-13-64-7d.

```
Switch_config# ip dhcpd pool test
Switch_config_dhcp# ip-bind 1.1.1.1 hardware-address 10-a0-0c-13-64-7d
```

The following example shows how to set the client ID of DHCP-manual-distribution address 1.1.1.2 to 01-10-a0-0c-13-64-7d.

```
Switch_config# ip dhcpd pool test
Switch_config_dhcp# ip-bind 1.1.1.2 identifier 01-10-a0-0c-13-64-7d
```

The following example shows how to set the host name of the manual-DHCP-distribution address 1.1.1.3 to Router-test.

```
Switch_config# ip dhcpd pool test
Switch_config_dhcp# ip-bind 1.1.1.3 host-name Router-test
```

3.2.9 hw-access deny

Syntax

To disable the DHCP service for specified hardware address, run the following command.

hw-access deny *hw-addr*

To return to the default setting, use the no form of this command.

no hw-access deny *hw-addr*

Parameters

Parameters	Description
hw-addr	*hw-addr* is used for the hardware address for disabling client device

Default Value

None

Command Mode

DHCP address pool configuration mode

Usage Guidelines

The command can be used to disable DHCP service for specified hardware address.

Example

The following example shows how to disable DHCP service for the hardware address 10:a0:0c:13:64:7d:

```
Switch_config# ip dhcpd pool test
Switch_config_dhcp# hw-access deny 10:a0:0c:13:64:7d
```

3.2.10 specific-information

Syntax

To configure DHCP server providing specified information for the client device, run the following command.

specific-information hex *hex-value*

To return to the default setting, use the no form of this command.

no specific-information hex

Parameters

Parameters	Description
hex-value	*hex-value* is used for DHCP server providing specified hexadecimal information for the client device

Default Value

None

Command Mode

DHCP address pool configuration mode

Usage Guidelines

The command can be used to configure DHCP server to provide the specified information for the client device.

Example

The following example shows how to configure DHCP sever to provide specified information for the client device:

```
Switch_config# ip dhcpd pool test
Switch_config_dhcp# specific-information hex 7d
```

3.2.11 class-identifier

Syntax

To provide DHCP service for the specified client device, run the following command.

class-identifier *WORD*

To return to the default setting, use the no form of this command.

no class-identifier

Parameters

Parameters	Description
WORD	*WORD* means the provider classification identifier which DHCP server applies to the client device.

Default Value

None

Command Mode

DHCP address pool configuration mode

Usage Guidelines

The command can be used to configure DHCP server to provide the specified information for the DHCP device.

Example

The following example shows how to configure the provider classification identifier which DHCP server applies to the client device to be BDCOM.

Switch_config# **ip dhcpd pool** *test*
Switch_config_dhcp# **class-identifier** *BDCOM*

3.3 DHCPD Debugging Commands

DHCPD Debugging Commands include:

- debug ip dhcpd packet
- debug ip dhcpd event
- debug ip dhcpd all

3.3.1 debug ip dhcpd packet

Syntax

To enable DHCPD data packet information output, run the following command.

debug ip dhcpd packet

To return to the default setting, use the no form of this command.

no debug ip dhcpd packet

Parameters

None

Default Value

None

Command Mode

Privileged mode

Usage Guidelines

The command is used to enable the debug OLT of the DHCPD packet's information.

Example

The following example shows how to enable the output OLT of the debugging information about the DHCPD packets.

Switch# **debug ip dhcpd packet**

3.3.2 debug ip dhcpd event

Syntax

To enable DHCPD event information output, run the following command.

debug ip dhcpd event

To return to the default setting, use the no form of this command.

no debug ip dhcpd event

Parameters

None

Default Value

None

Command Mode

Privileged mode

Usage Guidelines

The command is used to enable the debug OLT of the DHCPD event's information.

Example

The following example shows how to enable the output OLT of the debugging information about the DHCPD events.

```
Switch# debug ip dhcpd event
```

3.3.3 debug ip dhcpd all

Syntax

To enable DHCPD debug information output, run the following command.

debug ip dhcpd all

To return to the default setting, use the no form of this command.

no debug ip dhcpd all

Parameters

None

Default Value

None

Command Mode

Privileged mode

Usage Guidelines

You can use this command to enable the debug switch of the DHCPD event's information.

Example

The following example shows how to enable the output switch of the debugging information about the DHCPD events.

```
Switch# debug ip dhcpd all
```

3.4 DHCPD Management Commands

DHCPD Management Commands include:

- show ip dhcpd statistic
- show ip dhcpd binding
- clear ip dhcpd statistic
- clear ip dhcpd binding

3.4.1 show ip dhcpd statistic

Syntax

To display the DHCPD statistics information, run the following command.

show ip dhcpd statistic

Parameters

None

Default Value

None

Command Mode

All modes except the user mode

Usage Guidelines

You can use this command to display the DHCPD statistics information, including the quantity of all kinds of packets, and the number of manually or automatically distributed addresses.

Example

The following example shows how to display the DHCPD statistics information.

```
Switch_config# show ip dhcpd statistic
DHCP Server Statistic Information:   DHCP server packet statistic
  DHCP total packet                      0

  DHCP server DHCPDISCOVER          0
  DHCP server DHCPREQUEST                0
  DHCP server DHCPRELEASE               0
  DHCP server DHCPDECLINE               0
  DHCP server DHCPINFORM                0
  DHCP server DHCPOFFER                 0
  DHCP server DHCPACK                  0
  DHCP server DHCPNAK                  0

  DHCP relay bad packet            0
  DHCP relay server packet             0
  DHCP relay PC packet                  0
  DHCP relay STB packet                 0
  DHCP relay to server packet   0
  DHCP relay to client broadcast packet     0
  DHCP relay from client broadcast packet     0
  DHCP relay DHCPDISCOVER                   0
  DHCP relay DHCPREQUEST              0
  DHCP relay DHCPRELEASE              0
  DHCP relay DHCPDECLINE             0
  DHCP relay DHCPINFORM              0
  DHCP relay DHCPOFFER               0
  DHCP relay DHCPACK                0
  DHCP relay DHCPNAK                0

  BOOTP packet                               0
  DHCP error packet                        0

  max address number                   0
  max helper number                       0

  DHCP server binding statistic
  MANUALBIND                     0
  AUTOMATICBIND                  0
```

3.4.2 show ip dhcpd binding

Syntax

To show the address binding information of DHCPD, run the following command.

show ip dhcpd binding [*ip-addr*]&<0-10>

Parameters

Parameters	Description
ip-addr	Stands for the address of the to-be-displayed binding information.

Default Value

All address binding information is displayed.

Command Mode

All modes except the user mode

Usage Guidelines

You can use this command to display the address binding information, IP address, hardware address, bind-type and timeout time of DHCPD.

Example

The following example shows how to display the DHCPD binding information.

```
Switch_config# show ip dhcpd binding
```

3.4.3 clear ip dhcpd abandoned

Syntax

To delete the unavailable address information of DHCP Server, run the following command.

clear ip dhcpd abandoned

Parameters

None

Default Value

None

Command Mode

Privileged mode

Usage Guidelines

The command can be used to delete the unavailable address information of DHCP Server.

Example

The following example shows how to delete the unavailable address information of DHCP Server.

```
Switch# clear ip dhcpd abandoned
```

3.4.4 clear ip dhcpd statistic

Syntax

To delete the statistics information about the quantity of packets, run the following command.

clear ip dhcpd statistic

Parameters

None

Default Value

None

Command Mode

Privileged mode

Usage Guidelines

This command can be used to delete the statistics information about the quantity of packets.

Example

The following example shows how to delete the statistics information about the quantity of packets.

```
Switch# clear ip dhcpd statistic
```

3.4.5 clear ip dhcpd binding

Syntax

To delete the designated binding information, run the following command.

clear ip dhcpd binding {[*ip-addr*]&<0-10>|*}

Parameters

Parameters	Description
ip-addr	Stands for the address of the to-be-deleted binding information.
*	Means to delete all binding information.

Default Value

The designated binding information will be deleted by default.

Command Mode

Privileged mode

Usage Guidelines

This command can be used to delete the binding information of a designated address.

Example

The following example shows how to delete the binding information of 192.168.20.210.

```
Switch# clear ip dhcpd binding 192.168.20.210
```

The following example shows how to delete the binding information of 192.168.20.210 and 192.168.20.211.

```
Switch# clear ip dhcpd binding 192.168.20.210 192.168.20.211
```

The following example shows how to delete all binding information.

```
Switch# clear ip dhcpd binding *
```

Chapter 4 IPv6 Configuration Commands

4.1 IP Service Configuration Commands

IP Service Configuration Commands include:

- clear tcp
- clear tcp statistics
- debug arp
- debug ip icmp
- debug ip packet
- debug ip raw
- debug ip tcp packet
- debug ip tcp transactions
- debug ip udp
- ip mask-reply
- ip mtu
- ip redirects
- ip route-cache
- ip source-route
- ip tcp synwait-time
- ip tcp window-size
- ip unreachables
- show ip cache
- show ip irdp
- show ip sockets
- show ip traffic
- show tcp
- show tcp brief

- show tcp statistics
- show tcp tcb

4.1.1 clear tcp

Syntax

To clear a TCP connection, run the following command:

clear tcp {**local** *host-name port* **remote** *host-name port* **|** **tcb** *address* **|** **statistics** }

Parameters

Parameters	Description
local host-name port	IP address and TCP port of the local host
remote host-name port	IP address and TCP port of the remote host
tcb address	Address of the transmission control block (TCB) for the to-be-deleted TCP connection TCB is an internal identifier of the TCP connection, which can be obtained through the **show tcp brief** command.
statistics	TCP statistics

Command Mode

Privileged mode

Usage Guidelines

The clear tcp command is mainly used to delete the terminated TCP connection. The clear tcp command is mainly used to delete the terminated TCP connection. The TCP connection has no communication, so the system does not know that the TCP connection is already closed. In this case, the clear tcp command is used to close the invalid TCP connection. The clear tcp local host-name port remote host-name port command is used to close the TCP connection between the IP address or port of the local host and the IP address or port of the remote host. The clear tcp tcb address command is used to close the TCP connection identified by the designated TCB address.

Example

The following example shows that the TCP connection between 192.168.20.22:23 (local) and 192.168.20.120:4420 (remote). The show tcp brief command is used to display the information of the local and remote hosts of the current TCP connection.

```
switch# show tcp brief
```

```
TCB          Local Address        Foreign Address      State
0xE85AC8     192.168.20.22:23     192.168.20.120:4420  ESTABLISHED
0xEA38C8     192.168.20.22:23     192.168.20.125:1583  ESTABLISHED
switch# clear tcp local 192.168.20.22 23 remote 192.168.20.120 4420
switch# show tcp brief
TCB          Local Address        Foreign Address      State
0xEA38C8     192.168.20.22:23     192.168.20.125:1583  ESTABLISHED
```

The following example shows how to clear the TCP connection whose TCB address is 0xea38c8. The show tcp brief command displays the TCB address of the TCP connection.

```
switch#show tcp brief
TCB          Local Address        Foreign Address      State
0xEA38C8     192.168.20.22:23     192.168.20.125:1583  ESTABLISHED
switch# clear tcp tcb 0xea38c8
switch# show tcp brief
TCB          Local Address        Foreign Address      State
```

Related Command

show tcp

show tcp brief

show tcp tcb

4.1.2 clear tcp statistics

Syntax

To clear the statistics data about TCP, run the following command:

clear tcp statistics

Parameters

The command has no parameters or keywords.

Command Mode

Privileged mode

Example

The following example shows how to delete the TCP statistics information:

```
switch# clear tcp statistics
```

Related Command

show tcp statistics

4.1.3 debug arp

Syntax

To display the ARP interaction information, such as ARP request transmitting, ARP response receiving, ARP request receiving and ARP response transmitting, run debug arp. When the OLT and host cannot communicate with each other, you can run the command to analyze the ARP interaction information. You can run no debug arp to stop displaying the ARP interaction information.

debug arp [packet | delete]

no debug arp [packet | delete]

Parameters

The command has no parameters or keywords.

Command Mode

Privileged mode

Example

```
switch# debug arp
IP ARP: rcvd req src 192.168.20.116 00:90:27:a7:a9:c2, dst 192.168.20.111, vlan 10
IP ARP: req filtered src 192.168.20.139 00:90:27:d5:a9:1f, dst 192.168.20.82 00:
00:00:00:00:00, wrong cable, vlan 11
IP ARP: created an incomplete entry for IP address 192.168.20.77, vlan 10
IP ARP: sent req src 192.168.20.22 08:00:3e:33:33:8a, dst 192.168.20.77, vlan 10
IP ARP: rcvd reply src 192.168.20.77 00:30:80:d5:37:e0, dst 192.168.20.22, vlan 10
```

The first information line shows that the OLT receives an ARP request from Ethernet vlan 10. The ARP is sent from a host whose IP address is 192.168.20.116 and MAC address is 00:90:27:a7:a9:c2 and received by a host whose IP address is 192.168.20.111. The ARP request requires the MAC address of the destination host.

```
IP ARP: rcvd req src 192.168.20.116 00:90:27:a7:a9:c2, dst 192.168.20.111, vlan 10
```

The second information line shows that the OLT receives an ARP address request with IP 192.168.20.139 from interface Etherner vlan 11. However, according to the interface configuration of the OLT, the interface is not in the network claimed by the host. The reason may lie in the incorrect host configuration. If the OLT creates an ARP cache according to the information, it cannot communicate with a host having the same address though the host connects an interface normally.

```
IP ARP: req filtered src 192.168.20.139 00:90:27:d5:a9:1f, dst 192.168.20.82 00:
00:00:00:00:00, wrong cable, vlan 11
```

The third line shows that, before the OLT resolves the MAC address of host 192.168.20.77, an incomplete ARP item must be created in the ARP cache for the host; after the ARP response is received, the MAC address is entered. According to the configuration of the OLT, the host connects interface Ethernet vlan 10.

```
IP ARP: created an incomplete entry for IP address 192.168.20.77, vlan 10
```

The fourth information shows that the OLT transmits the ARP request from interface Ethernetvlan 10the IP addressof theOLT is192.168.20.22， the MAC addressofthe interface is 08:00:3e:33:33:8a08:00:3e:33:33:8aand the IP addressof the requested host is192.168.20.77. The four information line has connection with the third information line.

```
IP ARP: sent req src 192.168.20.22 08:00:3e:33:33:8a, dst 192.168.20.77, vlan 10
```

The fifth information line shows the OLT receivesthe ARP responsewhich istransferred from host 192.168.20.77 to the OLT’s interface19192.168.20.22 on interface Ethernet 1/0, telling thatthe MAC address is00:30:80:d5:37:e0. The fifth information line has connection with the third and fourth information lines.

```
IP ARP: rcvd reply src 192.168.20.77 00:30:80:d5:37:e0, dst 192.168.20.22, vlan 10
```

4.1.4 debug ip icmp

Syntax

To display the interaction information about ICMP, run the following command.

debug ip icmp

To disable the output of ICMP debug information, run the following command.

no debug ip icmp

Parameters

The command has no parameters or keywords.

Command Mode

Privileged mode

Usage Guidelines

The command is used to display the received and transmitted ICMP packets, helping to resolve the end-to-end connection problem. To understand the detailed meaning of the debug ip icmp command, see RFC 792, “Internal Control Message Protocol”.

Example

```
switch# debug ip icmp
ICMP: sent pointer indicating to 192.168.20.124 (dst was 192.168.20.22), len 48
```

```
ICMP: rcvd echo from 192.168.20.125, len 40
ICMP: sent echo reply, src 192.168.20.22, dst 192.168.20.125, len 40
ICMP: sent dst (202.96.209.133) host unreachable to 192.168.20.124, len 36
ICMP: sent dst (192.168.20.22) protocol unreachable to 192.168.20.124, len 36
ICMP: rcvd host redirect from 192.168.20.77, for dst 22.0.0.3 use gw 192.168.20.26, len 36
ICMP: rcvd dst (22.0.0.3) host unreachable from 192.168.20.26, len 36
ICMP: sent host redirect to 192.168.20.124, for dst 22.0.0.5 use gw 192.168.20.77, len 36
ICMP: rcvd dst (2.2.2.2) host unreachable from 192.168.20.26, len 36
```

The first information line is explained as follows:

ICMP: sent pointer indicating to 192.168.20.124 (dst was 192.168.20.22), len 48

Domain	Description
ICMP	Displays the information about ICMP
Sent	Transmits the ICMP packets.
pointer indicating	Type of the ICMP packet, which shows the original IP packet is incorrect and specifies the incorrect domain. Other types of ICMP packet include: echo reply (echo reply) dst unreachable including: ---net unreachable (net unreachable) ---host unreachable (host unreachable) ---protocol unreachable (protocol unreachable) ---port unreachable (port unreachable) ---fragmentation needed and DF set (fragmentation needed and DF set) ---source route failed (source route failed) ---net unknown (net unknown) ---destination host unknown (destination host unknown) ---source host isolated (source host isolated) ---net prohibited (net prohibited) ---host prohibited (host prohibited) ---net tos unreachable (net tos unreachable) ---host tos unreachable (host tos unreachable) source quench (source quench) redirect (redirection), including: ---net redirect (net redirect) ---host redirect (host redirect) ---net tos redirect (redirection for the service type and the network)

	---host tos redirect (redirection for the service type and the host) echo (echo request) router advertisement (OLT advertisement) router solicitation (OLT request) time exceeded (timeout), including: ---ttl exceeded (ttltimeout) ---reassembly timeout (reassembly timeout) parameter problem(parameter problem), including: ---pointer indicating (point error parameter) ---option missed (option missed) ---bad length (bad length) timestamp (timestamp) timestamp reply (timestamp reply) information request (information request) information reply (information reply) mask request (mask request) mask reply (mask reply) If it is the unknown ICMP type, the system will display the ICMP type and its code.
to 192.168.20.124	The destination address of the ICMP packet is 192.168.20.124, which is also the source address, of the original packet triggering the ICMP packet.
(dst was 192.168.20.22)	The destination address of the original packet leading to the ICMP packet is192.168.20.22.
len 48	The length of the ICMP packet is 48bytes, the length of IP header excluded.

The second information line is explained as follows:

ICMP: rcvd echo from 192.168.20.125, len 40

Domain	Description
rcvd	Receives the ICMPpacket.
echo	ICMPICMP packet type, Request response packet
from 192.168.20.125	ICMPThe source address of the ICMP packet is192.168.20.125.

The third information line is explained as follows:

ICMP: sent echo reply, src 192.168.20.22, dst 192.168.20.125, len 40

Domain	Command
src 192.168.20.22	ICMPThe source address of the ICMP packet is192.168.20.22.

dst 192.168.20.125	The destination address of the ICMP packet is 192.168.20.125.

Different types of ICMP packets have different formats when the ICMP packet is generated.

For example, the ICMP redirect packet adopts the following format:

```
ICMP: rcvd host redirect from 192.168.20.77, for dst 22.0.0.3 use gw 192.168.20.26, len 36
ICMP: sent host redirect to 192.168.20.124, for dst 22.0.0.5 use gw 192.168.20.77, len 36
```

The first information line shows that the redirect ICMP packet from host 192.168.20.77 is received and gateway 192.168.20.26 is recommended to forward the packet to destination host 22.0.0.3; the length of the ICMP packet is 36 bytes.

The second information line shows the redirect ICMP packet is sent to host 192.168.20.124. The redirect ICMP packet notifies the host of using gateway 192.168.20.77 to send packets to host 22.0.0.5. The length of the ICMP packet is 36 bytes.

For the DST unreachable ICMP packet, the following format is adopted for printing:

```
ICMP: sent dst (202.96.209.133) host unreachable to 192.168.20.124, len 36
ICMP: rcvd dst (2.2.2.2) host unreachable from 192.168.20.26, len 36
```

The first information line shows that, because the OLT cannot route a certain IP packet, the source host 192.168.20.124 sends the unreachable ICMP packet to the destination host (202.96.209.133). The length of the ICMP packet is 36 bytes.

The second information line shows that the OLT receives an ICMP packet from host 192.168.20.26, notifying that the destination host 2.2.2.2 cannot be reached. The length of the ICMP packet is 36 bytes.

4.1.5 debug ip packet

Syntax

To display the interaction information about IP, run the following command.

To return to the default setting, use the no form of this command.

debug ip packet [**detail | access-group** *ip-access-list-name* **| interface** *type number*]*

no debug ip packet

Parameters

Parameters	Description
detail	(optional) exports the protocol information encapsulated by the IP packet, such as the protocol number, number of the UDP port and the TCP port, and ICMP packet type.
ip-access-list-name	(optional) name of the IP ACL which is used to filter the output information Only the information about the IP packets that comply with the designated IP ACL can be exported.

interface	(optional) interface name which is used to filter the output information Only the information about the IP packets that comply with the designated port can be exported.

Command Mode

Privileged mode

Usage Guidelines

The command helps you to know the final destination of each received or locally-generated IP flows and to find the reason of the communication problem.

The following are potential cases:

- Forwarded
- Forwarded as the broadcast/multicast packet
- Failed addressing when the IP packet is forwarded
- Forwarding the redirect packet
- Rejected because of having the source route option
- Rejected because of illegal IP options
- Source route
- Locally-transmitted packets need fragmentation, while the DF bit is reset.
- Receiving the packets
- Receiving IP fragments
- Transmitting packets
- Transmitting the broadcast/multicast
- Failed addressing of locally-generated packets
- Locally-generated packets being fragmented
- Received packets being filtered
- Transmitted packets being filtered
- Encapsulation of the link layer failed (only for Ethernet)
- Unknown protocol

If you use the command, lots of output information will appear; you had better run the OLT at a relatively free time, or the system's performance may be badly affected.

Additionally, you had better filter the information output through the access list, enabling the system to display the information that interests users.

Example

```
switch# debug ip packet
switch#IP: s=192.168.20.120 (vlan 10), d=19.0.0.9 (vlan 10), g=192.168.20.1, len=60, redirected
IP: s=192.168.20.22 (local), d=192.168.20.120 (vlan 10), g=192.168.20.120, len=56, sending
IP: s=192.168.20.120 (vlan 10), d=19.0.0.9 (vlan 10), g=192.168.20.1, len=60, forward
IP: s=192.168.20.81 (vlan 10), d=192.168.20.22 (vlan 10), len=56, rcvd
```

Domain	Description
IP	Means that the information is about the IP packet.
s=192.168.20.120 (vlan 10)	Source address of the IP packet and the name of the interface receiving the packet
d=19.0.0.9 (vlan 10)	Destination address of the IP packet and the name of the interface transmitting the packet (if the routing succeeds)
g=192.168.20.1	Destination address of the next hop of the IP packet, which may be the gateway address or the destination address
len	Length of the IP packet
redirected	Means the OLT will send the ICMP redirected packet to the source host of the ICMP packet. The following are other cases: Forward—the packet is forwarded. forward directed broadcast---Packets are forwarded as the directed broadcast and packets will be transformed as the physical broadcast on the transmission interface unroutable---The addressing of the packet fails and the packet will be dropped. source route---Source route rejected source route---Because the system does not support the source route, the packets with the IP source route are rejected. Bad options—the IP option is incorrect and the packet will be dropped. need frag but DF set---The local packet need be fragmented; however, the DF is reset. rcvd---the packet is received by the local host. rcvd fragment---The fragment of the packet is received. sending---The locally-generated packet is being sent. sending broad/multicast---The locally-generated broadcast/multicast packet is being sent. sending fragment---The locally-fragmented IP packet is being

	sent. denied by in acl---The packet is denied by the ACL of the receiver interface. denied by out acl---The packet is denied by the transmitter interface. unknown protocol---unknown protocol encapsulation failed---the protocol encapsulation fails in the Ethernet. When the to-be-transmitted packet is dropped on the Ethernet interface because of ARP resolution failure, the information appears.

The first information line shows that the OLT has received an IP packet; its source address is 192.168.20.120 and destination address is 19.0.0.9; it is from the network segment connected by interface vlan 10; the transmitter interface determined by the routing table is interface vlan 10; the gateway's address is 192.168.20.1 and the length of the packet is 60 bytes. The gateway and the source host which transmits the IP packet are connected on the same network, that is, the network connected by interface vlan 10 of the switch. Hence, the OLT transmits the ICMP redirect packet.

```
IP: s=192.168.20.120 (vlan 10), d=19.0.0.9 (vlan 10), g=192.168.20.1, len=60, redirected
```

The second information line describes the transmission of the ICMP redirect packet. The source address is the local address 192.168.20.22 and the destination address is the source address of the previous packet, that is, 192.168.20.120. The ICMP redirect packet is transmitted from interface vlan 10 to the destination directly, so the address of the gateway is the destination address 192.168.20.120. The length of the ICMP redirect packet is 56 bytes.

```
IP: s=192.168.20.22 (local), d=192.168.20.120 (vlan 10), g=192.168.20.120, len=56, sending
```

The third information line shows that the IP layer receives an IP packet. The source address of the packet is 192.168.20.120; the transmitter interface is interface vlan 10; the destination address of the packet is 19.0.0.9. Through the routing table, the packet is found to forward to interface VLAN 10; the address of the gateway is 192.168.20.77 and the length of the packet is 60 bytes. This information shows the packet displayed when forwarding the first information after the system sends ICMP redirection packets.

```
IP: s=192.168.20.120 (vlan 10), d=19.0.0.9 (vlan 10), g=192.168.20.77, len=60, forward
```

The fourth information line shows that the IP layer receives an IP packet. The source address is 192.168.20.81 and the receiver interface is VLAN 10; the destination address is 192.168.20.22, which is an IP address configured on interface VLAN 10 of the OLT; the length of the packet is 56 bytes.

```
IP: s=192.168.20.81 (vlan 10), d=192.168.20.22 (vlan 10), len=56, rcvd
```

The output of the debug ip packet detail command is described in the following. Only newly-added parts are described.

```
switch# debug ip packet detail
switch#IP: s=192.168.12.8 (vlan 10), d=255.255.255.255 (vlan 10), len=328, rcvd, UDP: src=68, dst=67
IP: s=192.168.20.26 (vlan 10), d=224.0.0.5 (vlan 10), len=68, rcvd, proto=89
IP: s=192.168.20.125 (vlan 10), d=192.168.20.22 (vlan 10), len=84, rcvd, ICMP: type=0, code = 0
```

```
IP: s=192.168.20.22 (local), d=192.168.20.124 (vlan 10), g=192.168.20.124, len=40, sending,
TCP: src=1024, dst=23, seq=75098622, ack=161000466, win=17520, ACK
```

Domain	Description
UDP	Protocol name, such as UDP, ICMP or TCP. Other protocols are presented with the protocol number.
type, code	Type and code of the ICMP packet
src, dst	Source port and destination port of the UDP/TCP packet
seq	Sequence number of the TCP packet
ack	Acknowledge number of the TCP packet
win	Windows value of the TCP packet
ACK	ACK in the control bit of the TCP packet is reset, indicating that the acknowledge number is valid. Other control bits include SYN, URG, FIN, PSH and RST.

The first information line shows that the UDP packet is received. The source port is 68 and the destination port is 67.

```
IP: s=192.168.12.8 (vlan 10), d=255.255.255.255 (vlan 10), len=328, rcvd, UDP: src=68, dst=67
```

The second information line shows that the protocol number of the received packet is 89.

```
IP: s=192.168.20.26 (vlan 10), d=224.0.0.5 (vlan 10), len=68, rcvd, proto=89
```

The third information line shows that the ICMP packet is received. Both the packet type and the code are 0.

```
IP: s=192.168.20.125 (vlan 10), d=192.168.20.22 (vlan 10), len=84, rcvd, ICMP: type=0, code = 0
```

The fourth information line shows that the TCP packet is transmitted. The source port is 1024, the destination port is 23, the sequence number is 75098622, the acknowledge number is 161000466, the size of the receiver window is 17520 and the ACK bit is reset. For the meanings of these domains, see RFC 793— TRANSMISSION CONTROL PROTOCOL.

```
IP: s=192.168.20.22 (local), d=192.168.20.124 (vlan 10), g=192.168.20.124, len=40, sending,
TCP: src=1024, dst=23, seq=75098622, ack=161000466, win=17520, ACK
```

The following describes how to use the ACL. For example, to display the information about the packet whose source address is 192.168.20.125, you need to define the abc ACL and then allow the IP packets whose source address is 192.168.20.125. At last, you can use the ACL in the debug ip packet command.

```
switch# config
switch_config# ip access-list standard abc
switch_config_std_nacl# permit 192.168.20.125
switch_config_std_nacl# exit
switch_config#exit
switch#debug ip packet abc
switch#IP: s=192.168.20.125 (vlan 101), d=192.168.20.22 (vlan 101), len=48, rcvd
```

In the previous commands, the standard ACL is used. However, the expanded ACL can also be used.

Related Command

debug ip tcp packet

4.1.6 debug ip raw

Syntax

To display the interaction information about IP, run the following command. To return to the default setting, use the no form of this command.

debug ip raw [detail | access-group *ip-access-list-name* | interface *type number*]*

no debug ip raw

Parameters

Parameters	Description
detail	(optional) exports the protocol information encapsulated by the IP packet, such as the protocol number, number of the UDP port and the TCP port, and ICMP packet type.
access-list-group	(optional) name of the IP ACL which is used to filter the output information Only the information about the IP packets that comply with the designated IP ACL can be exported.
interface	(optional) interface name which is used to filter the output information Only the information about the IP packets that comply with the designated port can be exported.

Command Mode

Privileged mode

Usage Guidelines

The command helps you to know the final destination of each received or locally-generated IP flows and to find the reason of the communication problem.

The following are potential cases:

- Forwarded
- Forwarded as the broadcast/multicast packet
- Failed addressing when the IP packet is forwarded
- Forwarding the redirect packet

- Rejected because of having the source route option
- Rejected because of illegal IP options
- Source route
- Locally-transmitted packets need fragmentation, while the DF bit is reset.
- Receiving the packets
- Receiving IP fragments
- Transmitting packets
- Transmitting the broadcast/multicast
- Failed addressing of locally-generated packets
- Locally-generated packets being fragmented
- Received packets being filtered
- Transmitted packets being filtered
- Encapsulation of the link layer failed (only for Ethernet)
- Unknown protocol

If you use the command, lots of output information will appear; you had better run the OLT at a relatively free time, or the system's performance may be badly affected. Additionally, you had better filter the information output through the access list, enabling the system to display the information that interests users.

Example

It is the same with debug ip packet, so it is omitted here.

Related Command

debug ip tcp packet

4.1.7 debug ip tcp packet

Syntax

To display the information about receiving and transmitting the TCP packet, run debug ip tcp packet. To return to the default setting, use the no form of this command.

debug ip tcp packet

no debug ip tcp packet

Parameters

The command has no parameters or keywords.

Command Mode

Privileged mode

Usage Guidelines

None

Example

```
switch# debug ip tcp packet
tcp: O ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 50659460
      DATA 1 ACK 3130379810 PSH WIN 4380
tcp: I ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 3130379810
      DATA 2 ACK 50659460 PSH WIN 16372
tcp: O ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 50659461
      DATA 50 ACK 3130379812 PSH WIN 4380
tcp: O FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 50659511
      ACK 3130379812 FIN WIN 4380
tcp: I FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
      ACK 50659511 WIN 16321
tcp: I FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
      ACK 50659512 WIN 16321
tcp: I FIN_WAIT_2 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
      ACK 50659512 FIN WIN 16321
tcp: O TIME_WAIT 192.168.20.22:23 192.168.20.125:3828 seq 50659512
      ACK 3130379813 WIN 4380
tcp: I LISTEN 0.0.0.0:23 0.0.0.0:0 seq 3813109318
      DATA 2 ACK 8057944 PSH WIN 17440
tcp: O LISTEN 0.0.0.0:23 0.0.0.0:0 seq 8057944
      RST
```

Domain	Description
tcp:	Information about the TCP packets
O	Transmits the TCP packets.
ESTABLISHED	TCP Current state of the TCP connection For the description of the TCP connection's state, see the description of the debug ip tcp transactions command.
192.168.20.22:23	The source address of the packet is 192.168.20.22 and the source port is 23.

192.168.20.125:3828	The destination address of the packet is 192.168.20.125 and the destination port is3828.
seq 50659460	The sequence number of the packet is50659460.
DATA 1	Means that the packet contains only one effective byte.
ACK 3130379810	The acknowledgment number of the packet is 3130379810.
PSH	PSH is reset in the control bit of the packet. Other control bytes include ACK, FIN, SYN, URG and RST.
WIN 4380	Window domain of the packet used to notify the peer end to receive the cache size, which is 4380 bytes currently4380bytes
I	Receives the TCP packet.

If a domain of the previous domains does not appear, the domain has no effective value in the TCP packet.

Related Command

debug ip tcp transactions

4.1.8 debug ip tcp transactions

Syntax

To display the interaction information about TCP, run the following command.

debug ip tcp transactions

To return to the default setting, use the no form of this command.

no debug ip tcp transactions

Parameters

The command has no parameters or keywords.

Command Mode

Privileged mode

Example

```
switch# debug ip tcp transactions
TCP: rcvd connection attempt to port 23
TCP: TCB 0xE88AC8 created
TCP: state was LISTEN -> SYN_RCVD [23 -> 192.168.20.125:3828]
TCP: sending SYN, seq 50658312, ack 3130379657 [23 -> 192.168.20.125:3828]
```

```
TCP: state was SYN_RCVD -> ESTABLISHED [23 -> 192.168.20.125:3828]
TCP: connection closed by user, state was LISTEN [23 -> 0.0.0.0:0]
TCP: state was TIME_WAIT -> CLOSED [23 -> 192.168.20.125:3827]
TCP: TCB 0xE923C8 deleted
TCP: TCB 0xE7DBC8 created
TCP: connection to 192.168.20.124:513 from 192.168.20.22:1022, state was CLOSED to SYN_SENT
TCP: sending SYN, seq 52188680, ack 0 [1022 -> 192.168.20.124:513]
TCP: state was SYN_SENT -> ESTABLISHED [1022 -> 192.168.20.124:513]
TCP: rcvd FIN, state was ESTABLISHED -> CLOSE_WAIT [1022 -> 192.168.20.124:513]
TCP: connection closed by user, state was CLOSE_WAIT [1022 -> 192.168.20.124:513]
TCP: sending FIN [1022 -> 192.168.20.124:513]
TCP: connection closed by user, state was LAST_ACK [1022 -> 192.168.20.124:513]
TCP: state was LAST_ACK -> CLOSED [1022 -> 192.168.20.124:513]
TCP: TCB 0xE7DBC8 deleted
```

Domain	Description
TCP:	Displays the TCP interaction information.
rcvd connection attempt to port 23	Receives the connection request from the peer port23 (that is, the TELNET port.
TCB 0xE88AC8 created	Generates a new control block for the TCP connection, which is identified as 0xE88AC8.
state was LISTEN -> SYN_RCVD	Means that the TCP state machine changes from LISTEN to SYN_RCVD. The states of TCP include:: LISTEN---waiting for the TCP connection request from any remote host SYN_SENT---Sending out the connection request to trigger the TCP connection negotiation and then waiting for the peer's response SYN_RCVD—receiving the connection request from the peer, sending out the acknowledgment response and also sending out its connection request, and waiting for the connection request acknowledgment from the peer. ESTABLISHED---means that the connection is created; the connection is in the data transmission phase; the data of the upper-layer application can be received and transmitted. FIN_WAIT_1—Means that the connection termination request has been transmitted and the response and connection termination request from the peer are being waited. FIN_WAIT_2—Means that the connection termination request has been transmitted and the response from the peer has been received, while the connection termination request from the peer is being waited. CLOSE_WAIT—Means the connection termination request of

	the peer is received and the local response has been sent out, and now the local user is being waited to close the connection. Once the user requires closing the connection, the system will send the connection termination request. CLOSING—Means the connection termination request has been sent to the peer and the peer's connection termination request is also received and the corresponding response is also sent out, and now is waiting for the peer to acknowledge the local connection termination request. LAST_ACK—Means that the connection termination request from the peer is received and acknowledged, and now the connection termination request is transmitted and the response is waited. TIME_WAIT—Means that a sufficient time is needed to ensure that the peer has already received the local acknowledgement of the peer's connection termination request and the connection packet still being transmitted in the network is waited to be sent to the destination or be dropped. CLOSED—Means that there is no connection or the connection has been completed shut down. For more detailed information, see RFC 793, TRANSMISSION CONTROL PROTOCOL.
[23 -> 192.168.20.125:3828]	The content in the bracket is explained as follows: The first domain 23 stands for the local TCP port. The second domain(192.168.20.125)stands for the remote IP address. The third domain(3828)stand for the remote TCP port.
sending SYN	Transmits a connection request out (the SYN of the control bit in the TCP header is reset). Other TCP control bits include SYN, ACK, FIN, PSH, RST and URG.
seq 50658312	The sequence number of the transmitted packet is 50658312.
ack 3130379657	The acknowledgement number of the transmitted packet is 3130379657.
rcvd FIN	Means that the connection termination request is received (FINin the control bit of the TCP header is reset).
connection closed by user	Means that the upper-layer application requires disabling the TCP connection.
connection timed out	Means that the connection is closed because it times out.

Related Command

debug ip tcp packet

4.1.9 debug ip udp

Syntax

To display the interaction information about UDP, run the following command.

debug ip udp

To return to the default setting, use the no form of this command.

no debug ip udp

Parameters

The command has no parameters or keywords.

Command Mode

Privileged mode

Example

```
switch# debug ip udp
UDP: rcvd src 192.168.20.99(520), dst 192.168.20.255(520), len = 32
UDP: sent src 192.168.20.22(20001), dst 192.168.20.43(1001), len = 1008
```

Domain	Description
UDP:	Means that the information is about the UDP packet.
rcvd	Receiving the packets
sent	Means that the packet is transmitted.
src	Stands for the source IP address and UDP port of the UDP packet.
dst	Stands for the destination IP address and UDP port of the UDP packet.
len	Stands for the length of UDP packet.

The first information shows that the UDP packet is received. Its source address is 192.168.20.99 and its source port is port 520; its destination address is 192.168.20.255 and its destination port is port 520; the length of the packet is 32 bytes.

The second information shows that the UDP packet is transmitted. Its source address is 192.168.20.22 and its source port is port 20001; its destination address is 192.168.20.43 and its destination port is port 1001; the length of the packet is 1008 bytes.

4.1.10 ip mask-reply

Syntax

To enable the OLT to answer the request of the IP mask on the designated interface, run ip mask-reply.

ip mask-reply

To disable the OLT to answer the request of the IP mask on the designated interface, run the following command.

no ip mask-reply

To set OLT to reply IP address mask request on the designated interface, run the following command.

default ip mask-reply

Parameters

The command has no parameters or keywords.

Default Value

The IP mask request is not answered.

Command Mode

VLAN interface configuration mode

Example

```
Switch_config# interface vlan 11
Switch_config_v11# ip mask-reply
```

4.1.11 ip mtu

Syntax

To set the MTU of the IP packet transmitted from an interface, run the following command.

ip mtu *bytes*

To set the MTU of the IP packet transmitted from an interface as the default value, run the following command.

no ip mtu

default ip mtu

Parameters

Parameters	Description
bytes	Maximum IP transmission length which is counted with bytes

Default Value

The physical media of the interfaces are different, while the MTU on the interfaces are same. Sixty-eight bytes is the minimum MTU.

Command Mode

VLAN interface configuration mode

Usage Guidelines

If the length of the IP message exceeds IP MTU configured on the interface, the OLT fragments the message. All devices connecting on the same physical media need be configured the same MTU. The MTU affects the IP MTU. If the value of IP MTU is the same as that of the MTU, the value of IP MTU automatically changes to the new value of the MTU when the MTU value changes. The change of the IP MTU does not affect the MTU.

The minimum value of IP MTU is 68 bytes and the maximum value of IP MTU cannot exceed the MTU value configured on the interface.

Example

The following example shows that IP MTU on interface vlan 10 is set to 200:

```
Switch_config# interface vlan 10
Switch_config_v10# ip mtu 200
```

Related Command

mtu

4.1.12 ip redirects

Syntax

To send IP ICMP redirection packet, run the following command.

[no] ip redirects

To send IP ICMP redirection packet as the default setting, run the following command.

default ip redirects

Parameters

The command has no parameters or keywords.

Default Value

In general, the IP redirect packet is transmitted by default. However, the function that the IP redirect packet can be transmitted will be automatically disabled if the hot-standby OLT protocol is configured on the interface. If the configuration of the hot-standby OLT protocol is canceled later, the function cannot be automatically enabled.

Command Mode

VLAN interface configuration mode

Usage Guidelines

When the OLT detects that the forwarding interface of the gateway is the same as that of the received packet during the transmission of packets and if the packet-transmitting host directly connects the logic network of the interface, the OLT can transmit an ICMP redirect packet according to the protocol, notifying the source host of directly taking that OLT as the gateway for the destination address of the packet without packet forwarding through this OLT.

If the hot-standby OLT protocol is configured on an interface, the transmission of IP redirect packet may cause the loss of the packet.

Example

The following example shows how to enable the function of transmitting the ICMP redirect passage on interface vlan 10:

```
Switch_config# interface vlan 10
Switch_config_v10# ip redirects
```

4.1.13 ip route-cache

Syntax

To enable the routing cache, run the following command.

[no] ip route-cache

[no] ip route-cache same-interface

To return to the default setting, use the no form of this command.

default ip route-cache

Parameters

Parameters	Description
same-interface	Allows the IP packet to be rapidly forwarded from the received interface.

Default Value

Fast switching is allowed on an interface, while fast switching is forbidden on the same interface.

Command Mode

VLAN interface configuration mode

Usage Guidelines

The route cache can conduct the load balance to the forwarded packets based on the source/destination address.

If the route cache is enabled, the packet forwarding rate of the OLT will be improved. However, the route cache should be forbidden on the low-speed line (64k or even less than 64k).

You can run ip route-cache same-interface to allow rapid IP switching on the same interface, that is, the receiver interface is same to the transmitter interface. In general, the function is not recommended to be enabled because the function conflicts with the redirect function of the OLT. If you has a incompletely-connected network, such as a frame-relay network, you can enable the function on the frame-relay interface. For example, in a frame-relay network consisting of OLT A, B and C, there are only links from A to B and from B to C, the communication between OLT A and OLT C must be forwarded through OLT B. In this case, OLT B receives a packet from OLT A through a DLCI of an interface, and then transmits the packet to OLT C through another DLCI of the same interface.

Example

The following command is used to allow fast switching on the same interface.

```
Switch_config# interface vlan 10
Switch_config_v10# ip route-cache same-interface
```

The following command is used to forbid fast switching even on the same interface.

```
Switch_config# interface vlan 10
Switch_config_v10# no ip route-cache
```

The following command is used to forbid fast switching only on the same interface.

Switch_config# **interface vlan** *10*

Switch_config_v10# **no ip route-cache same-interface**

The following command is used to enable the default setting (allowing fast switching, the same interface excluded).

Switch_config# **interface vlan** *10*

Switch_config_v10# **ip route-cache**

Related Command

show ip cache

4.1.14 ip route-cache hit-numbers

Syntax

To set the hit numbers of adding the item of the software route cache to that of the hardware route cache, run the following command.

ip route-cache hit-numbers *hit-number*

To return to the default setting, use the no form of this command.

no ip route-cache hit-numbers

Parameters

Parameters	Description
hit-number	Sets the hit numbers of adding the item of the software route cache to that of the hardware route cache. The value ranges from 1 to 10.

Default Value

The default value is 5.

Command Mode

Global configuration mode

Usage Guidelines

The command is used to set the hit numbers of adding the item of the software route cache to that of the hardware route cache.

Example

The following example shows to add the item in the software route cache which has been hit twice to the hardware route cache.

```
Switch_config# ip route-cache hit-numbers 2
```

Related Command

show ip cache

4.1.15 ip route-cache age-exf

Syntax

To delete the hardware route of a host in case the next hop of the route of the indirectly connected host is same as that of a subnet route, run the following command:

[**no**] **ip route-cache age-exf**

Parameters

None

Default Value

It is enabled by default.

Command Mode

Global configuration mode

Usage Guidelines

In case the next hop of the route of the indirectly connected host is same as that of a subnet route, the command will be used to decide whether to delete the hardware route of a host.

Example

After the no ip exf command is run in global mode, the dst:192.200.1.1 nh:192.3.3.2 route of the indirectly connected host will be generated due to the forwarding of L3 packets. If you want to enable IP EXF globally in this case, two results, as shown below, will be obtained according to the shutdown or opening of ip route-cache age-exf.

a. If the ip route-cache age-exf command is enabled, the hardware subnet route, dst:192.200.1.0/24 nh:192.3.3.2, will be generated and at the same time the hardware host’s route, dst:192.200.1.1 nh:192.3.3.2, will be deleted.

b. If the ip route-cache age-exf command is disabled, the hardware subnet route, dst:192.200.1.0/24 nh:192.3.3.2, will be generated and at the same time the hardware host’s route, dst:192.200.1.1 nh:192.3.3.2, will be kept.

Related Command

ip exf

show ip cache

4.1.16 ip route-cache cache-pbr

Syntax

To add hosts which is found through some policy routes to the hardware host table, run the following command. To return to the default setting, use the no form of this command.

ip route-cache cache-pbr

[**no**] **ip route-cache cache-pbr**

Parameters

None

Default Value

Disabled

Command Mode

Global configuration mode

Usage Guidelines

After the policy routing is set, those route caches that look for routes through the policy routing cannot be added to the hardware table, and in this case the software forwarding reduces in its performance; after this command is set, these route caches can be added to the hardware table to improve the performance of the system.

Example

The following example shows how to enable the function in global mode:

```
Switch_config# ip route-cache cache-pbr
```

Related Command

show ip cache

4.1.17 ip route-cache age-delay

Syntax

To set the delay of route hardware cache, run the following command.

ip route-cache age-delay *age-delay*

To return to the default setting, use the no form of this command.

no ip route-cache age-delay

Parameters

Parameters	Description
age-delay	Sets the delay of route hardware cache. The value ranges from 0 to 90.

Default Value

The default value is 0.

Command Mode

Global configuration mode

Usage Guidelines

If the delay is set, the related hardware route cache will be kept from being deleted promptly at the change of ARP until the delay is done. The greater the delay, the longer it is.

Note: In a network with a lot of directly connected hosts, ARP change will lead to the cancellation of related hardware route cache, leaving here a lot of packets to impact CPU, while the delay settings can provide a temporary protection to CPU. This command is always used together with another command, arp retry-allarp, and when both commands are executed, the system will learn ARP again and then reset the correct egress for IP cache as soon as possible.

Example

The following example shows how to set the delay of hardware route cache, which is caused by ARP change, to 60:

```
Switch_config# ip route-cache age-delay 60
```

Related Command

show ip cache

4.1.18 ip route-cache softcache-alive-time

Syntax

To set the lifetime of the entries in the software route cache, run the following command.

ip route-cache softcache-alive-time *alive-time*

To return to the default setting, use the no form of this command.

no ip route-cache softcache-alive-time

Parameters

Parameters	Description
alive-time	Stands for the lifetime of the route entries in the software cache, whose unit is 10ms. The value ranges from 1000 to 5000.

Default Value

The default value of the lifetime is 3000, that is, 30s.

Command Mode

Global configuration mode

Usage Guidelines

This command is used to set the lifetime of the entries in the software route cache.

Example

The following example shows how to set the lifetime of the entries in the software route cache to 40s:

```
Switch_config# ip route-cache softcache-alive-time 4000
```

Related Command

show ip cache

4.1.19 ip route-cache software-index

Syntax

To set the maximum time for the timer to operate the entries in the software route cache, run the following command.

ip route-cache software-index *ticks*

To return to the default setting, use the no form of this command.

no ip route-cache software-index

Parameters

Parameters	Description
ticks	Sets the maximum time for the timer to operate the entries in the software route cache each time. The value ranges from 1 to 100.

Default Value

The default value of the lifetime is 1, that is, 10ms.

Command Mode

Global configuration mode

Usage Guidelines

This command is used to set the maximum time for the timer to operate the entries in the software route cache. The bigger the maximum time is, the sooner the invalid software route cache ages, especially when the system is busy. Hence, this command can be used to restrain the quantity of the invalid entries in the software route cache.

Example

The following example shows how to set the maximum time, which is for the timer to operate the entries in the software route cache, to 500ms:

```
Switch_config# ip route-cache software-index 50
```

Related Command

show ip cache

4.1.20 ip route-cache hardware-index

Syntax

To set the maximum time for the timer to operate the entries in the hardware route cache, run the following command.

ip route-cache hardware-index *ticks*

To return to the default setting, use the no form of this command.

no ip route-cache hardware-index

Parameters

Parameters	Description
ticks	Sets the maximum time for the timer to operate the entries in the software route cache each time. The value ranges from 1 to 100.

Default Value

The default value of the lifetime is 50, that is, 0.5s.

Command Mode

Global configuration mode

Usage Guidelines

This command is used to set the maximum time for the timer to operate the entries in the hardware route cache. The bigger the maximum time is, the sooner the invalid hardware route cache ages, especially when the system is busy.

Example

The following example shows how to set the maximum time, which is for the timer to operate the entries in the software route cache, to 600ms:

```
Switch_config# ip route-cache hardware-index 60
```

Related Command

show ip cache

4.1.21 ip route-cache-aging-time

Syntax

To set the lifetime of the entries in the hardware route cache, run the following command.

ip route-cache-aging-time *seconds*

To return to the default setting, use the no form of this command.

no ip route-cache-aging-time

Parameters

Parameters	Description
seconds	The survival time of hardware routing cache. The value ranges from 0, 10 to 1000000.

Default Value

The default value is 300s.

Command Mode

Global configuration mode

Usage Guidelines

This command is used to set the lifetime of the entries in the hardware route cache.

Example

The following example shows how to set the lifetime of the entries in the hardware route cache to 600s:

```
Switch_config# ip route-cache-aging-time 600
```

Related Command

show ip cache

4.1.22 ip source-route

Syntax

To set the lifetime of the entries in the hardware route cache, run the following command. The IP packet with the source IP route option is dropped.

ip source-route

To drop any IP packet with IP source route option, run the following command.

no ip source-route

Parameters

None

Default Value

The IP packet with the source IP route option is handled.

Command Mode

Global configuration mode

Example

The following example shows how to enable the OLT to handle the IP packet with the source IP route option.

```
Switch_config# ip source-route
```

Related Command

ping

4.1.23 ip tcp synwait-time

Syntax

To set the timeout time for the OLT to wait for the successful TCP connection, run the following command. To return to the default setting, use the no form of this command.

ip tcp synwait-time *seconds*

no ip tcp synwait-time

Parameters

Parameters	Description
seconds	Time for the TCP connection, whose unit is second. The valid vale ranges between 5 and 300 seconds. The default value is 75.

Default Value

75 seconds

Command Mode

Global configuration mode

Usage Guidelines

When the OLT triggers the TCP connection and if the TCP connection is not established in the designated wait time, the OLT views that the connection fails and then sends the result to the upper-layer program. You can set the wait time for creation of the TCP connection. The default value of the wait time is 75 seconds. The option has no relation with the TCP connection packet which is forwarded through the OLT, but has relation with the TCP connection of the OLT itself.

Example

The following example shows how to set the wait time of creating TCP connection to 30 seconds:

```
switch_config# ip tcp synwait-time 30
```

4.1.24 ip tcp window-size

Syntax

To set the size of TCP windows, run the following command.

ip tcp window-size *bytes*

To return to the default setting, use the no form of this command.

no ip tcp window-size

Parameters

Parameters	Description
bytes	Size of the window The maximum window size is 65535 bytes. The default window size is 2000 bytes.

Default Value

2000 bytes

Command Mode

Global configuration mode

Usage Guidelines

Do not change the window size at will unless you have a definite purpose.

Example

The following example shows how to set the size of the TCP window to 6000 bytes.

```
switch_config# ip tcp window-size 6000
```

4.1.25 ip unreachables

Syntax

To enable the OLT to transmit the ICMP unreachable packet, run the following command. To return to the default setting, use the no form of this command.

ip unreachables

no ip unreachables

Parameters

The command has no parameters or keywords.

Default Value

ICMP unreachable packets are sent by default.

Command Mode

VLAN interface configuration mode

Usage Guidelines

When the OLT forwards the IP packet, the packet may be dropped because there is no relative route in the routing table. In this case, the OLT can send the ICMP unreachable packet to the source host, notifying the source host and enabling it to detect the host timely and correct the fault rapidly.

Example

The following example shows how to enable the ICMP unreachable packet to be transmitted on interface vlan 10:

```
Switch_config# interface vlan 10
Switch_config_v10# ip unreachables
```

4.1.26 show ip cache

Syntax

To display the route cache which is used for fast IP switching, run this command.

show ip cache [*prefix mask* **|software|hardware | vlan** *number* **| summary**]

Parameters

Parameters	Description
prefix mask	(Optional) Displays the items whose destination addresses match up the designated prefixes/masks users enter.
software	(Optional) Displays the items whose transmitter interfaces match up the designated interface types/numbers users enter.
hardware	(Optional) Displays the items whose transmitter interfaces match up the designated interface types/numbers users enter.
vlan *number*	To display the route cache items belong to vlan, run the following command.
summary	Displays the route cache summary.

Command Mode

Other modes except the user mode

Example

The following example shows how to display route cache:

```
switch# show ip cache
Source            Destination       Interface       Next Hop
192.168.20.125   2.0.0.124         vlan 210        2.0.0.124
192.168.20.124   192.168.30.124    vlan 210        2.0.0.124
2.0.0.124        192.168.20.125    vlan 11      192.168.20.125
```

Domain	Description
Source	Source address
Destination	Destination address
Interface	Type and number of the transmitted interface
Next Hop	Gateway address

The following example shows the route cache whose destination address matches up the designated prefix/mask.

```
switch# show ip cache 192.168.20.0 255.255.255.0
Source            Destination       Interface        Next Hop
2.0.0.124         192.168.20.125    vlan 101         192.168.20.125
```

The following example shows the route cache whose transmitter interface matches up the designated interface type/mask.

```
switch# show ip cache vlan 210
Source            Destination       Interface        Next Hop
192.168.20.125    2.0.0.124         vlan 210         2.0.0.124
192.168.20.124    192.168.30.124    vlan 210         2.0.0.124
```

4.1.27 show ip irdp

Syntax

To show all irdp protocl information or irdp protocl information of the designated port, run the following command.

show ip irdp [interface *type number***]**

Parameters

Parameters	Description
type	(optional) interface type
number	(optional) interface number

Command Mode

Other modes except the user mode

Example

```
Switch_config# show ip irdp
Async0/0 ICMP router discovery protocol(IRDP) : OFF

vlan 10 ICMP router discovery protocol(IRDP) : ON
  Advertisements occur between every 450 and 600 seconds
  Advertisements are sent as broadcasts
  Advertisements valid in 1800 seconds
  Default preference : 0

vlan 11 ICMP router discovery protocol(IRDP) : OFF
Null0 ICMP router discovery protocol(IRDP) : OFF
Loopback7 ICMP router discovery protocol(IRDP) : OFF
Loopback10 ICMP router discovery protocol(IRDP) : OFF
```

4.1.28 show ip sockets

Syntax

To display the socket information, run the following command.

show ip sockets [*socketid* **]**

Parameters

Parameters	Description
socketid	Displays some socket information.

Command Mode

Other modes except the user mode

Example

```
switch# show ip sockets
```

Proto	Local	Port	Remote	Port	In	Out
17	0.0.0.0	0	0.0.0.0	0	161	0
6	0.0.0.0	0	0.0.0.0	0	513	0
17	0.0.0.0	0	0.0.0.0	0	1698	0
17	0.0.0.0	0	0.0.0.0	0	69	0
6	0.0.0.0	0	0.0.0.0	0	23	0
17	0.0.0.0	0	0.0.0.0	0	137	122590

Domain	Description
Proto(Protocol)	IPProtocol ID 17 meansUDP,6meansTCP.
Remote(Remote)	Remote address
Port(Port)	Remote port
Local(local)	Local address

Port(Port)	Local port
In(receive)	Total number of the received bytes
Out(send)	Total number of the received bytes

4.1.29 show ip traffic

Syntax

To display the IP flow statistics information, run the following command:

show ip traffic

Parameters

The command has no parameters or keywords.

Command Mode

Privileged mode

Example

```
switch# show ip traffic
IP statistics:
  Rcvd:   359 total, 296 local destination, 286 delivered
          1 format errors,0 ipInSrcErrors,   0 checksum errors, 0 bad hop count
          0 ip hdr too short errors,0 ip mlen tooshort errors
          0 bad destination address, 0 bad source address, 1 unknown protocol, 0
discarded
          0 filtered , 0 bad options, 9 with options
  Opts:   0 loose source route, 0 record route, 0 strict source route
          0 timestamp, 9 router alert, 0 other
  Frags: 0 fragments, 0 reassembled, 0 dropped
          0 fragmented, 0 fragments, 0 couldn't fragment
  Bcast: 287 received, 0 sent
  Mcast: 0 received, 0 sent
  Sent:   0 generated, 0 forwarded
          0 filtered, 0 no route, 0 nat-drops, 0 discarded, 0 encapsulation faile
d

ICMP statistics:
  Rcvd: 0 total, 0 format errors, 0 checksum errors
         0 redirect, 0 unreachable, 0 source quench
         0 echos, 0 echo replies, 0 mask requests, 0 mask replies
         0 parameter problem, 0 timestamps, 0 timestamp replies
```

```
            0 time exceeded, 0 router solicitations, 0 router advertisements
  Sent: 0 total, 0 errors, 0 bandwidth limit
            0 redirects, 0 unreachable, 0 source quench
            0 echos, 0 echo replies, 0 mask requests, 0 mask replies
            0 parameter problem, 0 timestamps, 0 timestamp replies
            0 time exceeded, 0 router solicitations, 0 router advertisements

UDP statistics:
  Rcvd: 286 total, 0 checksum errors, 286 no port, 0 full sock
  Sent: 0 total

TCP statistics:
  Rcvd: 0 total, 0 checksum errors, 0 no port, 0 check md5 authen fails, 0 add m
d5 authen fails
  Sent: 0 total

ARP statistics:
  Rcvd: 24 total, 24 requests, 0 replies, 0 reverse, 0 other
  Sent: 7 total, 0 requests, 7 replies (0 proxy), 0 reverse
```

Domain	Description
format errors (format errors)	Error of the packet's format, such as incorrect IP header length
bad hop count (TTLerror)	If the routing OLT finds that the TTL value of the packet decreases to zero when it forwards the packet. the packet will be dropped.
no route (no route)	Means that the OLT has no corresponding route.

4.1.30 show tcp

Syntax

To display all status information of TCP connection, run the following command.

show tcp

Parameters

The command has no parameters or keywords.

Command Mode

Other modes except the user mode

Example

```
switch# show tcp
TCB 0xE9ADC8
Connection state is ESTABLISHED, unread input bytes: 934
Local host: 192.168.20.22, Local port: 1023
Foreign host: 192.168.20.124, Foreign port: 513

Enqueued bytes for transmit: 0, input: 934   mis-ordered: 0 (0 packets)

Timer          Starts    Wakeups          Next(ms)
Retrans            33          1                 0
TimeWait            0          0                 0
SendWnd             0          0                 0
KeepAlive         102          0           7199500

iss:  29139463  snduna:  29139525  sndnxt:  29139525    sndwnd:     17520
irs: 709124039   rcvnxt: 709205436   rcvwnd:       4380

SRTT: 15 ms, RXT: 2500 ms, RTV: 687 ms
minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

Datagrams (max data segment is 1460 bytes):
Rcvd: 102 (out of order: 0), with data: 92, total data bytes: 81396
Sent: 104 (retransmit: 0), with data: 31, total data bytes: 61
```

Domain	Description
TCB 0xE9ADC8	Internalidentifier of the control block for the TCP connection
Connection state is ESTABLISHED	Current state of the TCP connection The TCP connection may be in one of the following states: LISTEN---Means the TCP connection request from any remote host is being waited. SYN_SENT---Means that the response from the peer is being waited after the connection request is transmitted to the peer. SYN_RCVD—receiving the connection request from the peer, sending out the acknowledgment response and also sending out its connection request, and waiting for the connection request acknowledgment from the peer ESTABLISHED---means that the connection is created; the connection is in the data transmission phase; the data of the upper-layer application can be received and transmitted. FIN_WAIT_1—Means that the connection termination request has been transmitted and the response and connection termination request from the peer are being waited. FIN_WAIT_2—Means that the connection termination request

	has been transmitted and the response from the peer has been received, while the connection termination request from the peer is being waited. CLOSE_WAIT—Means the connection termination request of the peer is received and the local response has been sent out, and now the local user is being waited to close the connection. Once the user requires closing the connection, the system will send the connection termination request. CLOSING—Means the connection termination request has been sent to the peer and the peer's connection termination request is also received and the corresponding response is also sent out, and now is waiting for the peer to acknowledge the local connection termination request. LAST_ACK—Means that the connection termination request from the peer is received and acknowledged, and now the connection termination request is transmitted and the response is waited. TIME_WAIT—Means that a sufficient time is needed to ensure that the peer has already received the local acknowledgement of the peer's connection termination request and the connection packet still being transmitted in the network is waited to be sent to the destination or be dropped. CLOSED—Means that there is no connection or the connection has been completed shut down. For more detailed information, see RFC 793, TRANSMISSION CONTROL PROTOCOL.
unread input bytes:	Data that is submitted to but not yet received by the upper-layer application after the lower-layer TCP handles
Local host:	Local IP address
Local port:	Local TCP port
Foreign host:	Remote IP address
Foreign port:	Remote TCP port.
Enqueued bytes for transmit:	Bytes in the transmission queue, including the transmitted but unacknowledged data bytes and not-yet-transmitted data bytes
input:	Data in the receiver queue which is waiting for being received by the upper-layer application after sorting
mis-ordered:	Number of bytes and number of packets in the mis-ordered queue. These data can enter the receiver queue in order and be received by the upper-layer application after other data is received. For example, if packets 1, 2, 23, 4, 5 and 6 are received, packets 1 and 2 can enter the receiver queue, while packets 4, 5 and 6 have to enter the mis-ordered queue to wait for the arrival of packet 3.

The information about the currently-displayed timer will then be displayed, including start-up times, timeout times and next timeout time (0 means the timer doesn't work currently). Each connection has its independent timers. The timeout times of the timer are generally less than the start-up times of the timer because the timer may be reset when it is running. For example, if the system receives the peer's acknowledgment of all transmitted data when the re-sending timer runs, the re-sending timer will stop running.

```
Timer        Starts   Wakeups        Next(ms)
Retrans         33         1            0
TimeWait         0         0            0
SendWnd          0         0            0
KeepAlive      102         0      7199500
```

Domain	Description
Timer	Name of the timer
Starts	Start-up times of the timer
Wakeups	Timeout times of the timer
Next(ms)	Time before next timeout occurs (unit: millisecond) 0 means that the timer is not running.
Retrans	Retransmission timer which is used to retransmit the data. The timer is restarted after the data is transmitted. If the data is not acknowledged by the peer during the timeout time, the data will be resent.
TimeWait	Time-wait timer which is used to ensure that the peer receives the acknowledgement of the connection termination request.
SendWnd	Timer of the transmission timer, used to ensure that the receiver window resumes the normal size after the TCP acknowledgment is lost.
KeepAlive	KeepAlive timer used to ensure that the communication link is normal and the peer is still in the connection state. It will trigger the transmission of the test packet to detect the state of the communication link and the peer's state.

The sequence number of the TCP connection will then be displayed. The reliable and ordered data transmission is guaranteed through the sequence number. The local/remote host conducts flow control and transmission acknowledgment through the sequence number.

```
iss:  29139463  snduna:  29139525  sndnxt:  29139525    sndwnd:     17520
irs: 709124039  rcvnxt: 709205436  rcvwnd:      4380
```

Domain	Description
iss:	Initial transmission sequence number
snduna:	Transmission sequence number of the first byte in the data which has been transmitted but the peer's acknowledgment is not received

sndnxt:	Transmission sequence number of the first byte in the data which will be transmitted next time
sndwnd:	Size of the TCP window of the remote host.
irs:	Initial reception sequence number, that is, initial transmission sequence number of the remote host
rcvnxt:	Recently-acknowledged acceptation sequence number
rcvwnd:	Size of the TCP window of the local host

The transmission time recorded by the local host is then displayed. The system can adapt to different networks according to the data.

```
SRTT: 15 ms, RXT: 2500 ms, RTV: 687 ms
minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms
```

Domain	Description
SRTT:	Round-trip time after smooth handle
RXT:	Retransmission timeout time
RTV:	Change value of the round-trip time
MinRXT:	Allowable minimum retransmission timeout
MaxRXT:	Allowable maximum retransmission timeout
ACK hold:	Maximum latency time for delaying the acknowledgment and enabling it to be transmitted together with the data

```
Datagrams (max data segment is 1460 bytes):
Rcvd: 102 (out of order: 0), with data: 92, total data bytes: 81396
Sent: 104 (retransmit: 0), with data: 31, total data bytes: 61
```

Domain	Description
max data segment is	Maximum data-segment length allowed by a connection
Rcvd:	Number of packets received by the local host through the connection and the number of mis-ordered packets
with data:	Number of packets which contains valid data
total data bytes:	Total data bytes contained in the packet
Sent	Total number of packets transmitted by the local host during the connection and the number of resent packets
with data:	Number of packets which contains valid data
total data bytes:	Total data bytes contained in the packet

Related Command

show tcp brief

show tcp tcb

4.1.31 show tcp brief

Syntax

To display the brief information about the TCP connection, run the following command:

show tcp brief [**all**]

Parameters

Parameters	Description
all	(optional) Displays all ports. If the keyword is not entered, the system will not display the port in listening mode.

Command Mode

Other modes except the user mode

Example

```
switch# show tcp brief
TCB            Local Address              Foreign Address           State
0xE9ADC8       192.168.20.22:1023       192.168.20.124:513       ESTABLISHED
0xEA34C8       192.168.20.22:23         192.168.20.125:1472      ESTABLISHED
```

Domain	Description
TCB	TCP Internal identifier of the TCP connection
Local Address	Local address and local TCP port
Foreign Address	IP address and TCP port of the remote host.
State	State of the connection For details, see the show tcp command.

Related Command

show tcp
show tcp tcb

4.1.32 show tcp statistics

Syntax

To display the statistics data about TCP, run the following command:

show tcp statistics

Parameters

The command has no parameters or keywords.

Command Mode

Other modes except the user mode

Example

```
switch# show tcp statistics
Rcvd: 148 Total, 0 no port
0 checksum error, 0 bad offset, 0 too short
131 packets (6974 bytes) in sequence
0 dup packets (0 bytes)
0 partially dup packets (0 bytes)
0 out-of-order packets (0 bytes)
0 packets (0 bytes) with data after window
0 packets after close
0 window probe packets, 0 window update packets
0 dup ack packets, 0 ack packets with unsend data
127 ack packets (247 bytes)
Sent: 239 Total, 0 urgent packets
6 control packets
123 data packets (245 bytes)
0 data packets (0 bytes) retransmitted
110 ack only packets (101 delayed)
0 window probe packets, 0 window update packets
4 Connections initiated, 0 connections accepted, 2 connections established
3 Connections closed (including 0 dropped, 1 embryonic dropped)
5 Total rxmt timeout, 0 connections dropped in rxmt timeout
1 Keepalive timeout, 0 keepalive probe, 1 Connections dropped in keepalive
```

Domain	Description
Rcvd:	Statistics data of the packets received by the OLT
Total	Total number of the received packets
no port	Number of received packets which have no destination ports
checksum error	Number of received packets which have checksum error
bad offset	Number of received packets which have offset error
too short	Number of received packets whose length is less than the valid effective length
packets in sequence	Number of packets received in order

dup packets	Number of received duplicate packets
partially dup packets	Number of some duplicate packets received
out-of-order packets	Number of packets received out of order
packets with data after window	Number of received packets whose data exceeds the received window of the OLT
packets after close	Number of packets received after the connection is closed
window probe packets	Number of received packets about window detection
window update packets	Number of received packets about window update
dup ack packets	Number of packets which are re-acknowledged after received
ack packets with unsent data	Number of packets which are received but not sent
ack packets	Number of acknowledgement packets
Sent	Statistics data of the packets received by the OLT
Total	Total number of the transmitted packets
urgent packets	Number of transmitted urgent packets
control packets	Total number of control packets (SYN , FIN or RSTwhich have been transmitted
data packets	Number of transmitted urgent packets
data packets retransmitted	Number of resent data packets
ack only packets	Number of transmitted acknowledgment packets
window probe packets	Number of transmitted packets about window detection
window update packets	Number of transmitted packets about window update
Connections initiated	Number of locally-initiated connections
connections accepted	Number of locally-accepted connections
connections established	Number of locally-established connections
Connections closed	Number of locally-closed connections
Total rxmt timeout	Total number of re-transmission timeouts
Connections dropped in rxmit timeout	Number of disconnected connections because of re-transmission timeout
Keepalive timeout	Number of keepalive timeouts
keepalive probe	Number of transmitted packets about keepalive detection
Connections dropped in keepalive	Number of connections which are disconnected because of Keepalive

Related Command

clear tcp statistics

4.1.33 show tcp tcb

Syntax

To display the state of a TCP connection, run the following command:

show tcp tcb *address*

Parameters

Parameters	Description
address	Address of the transmission control block (TCB) for the to-be-displayed TCP connection. TCB is an internal identifier of the TCP connection, which can be obtained through the show tcp brief command.

Command Mode

Other modes except the user mode

Example

The following information is displayed after the show tcp command is run:

switch_config# **show tcp tcb** *0xea38c8*

```
TCB 0xEA38C8
Connection state is ESTABLISHED, unread input bytes: 0
Local host: 192.168.20.22, Local port: 23
Foreign host: 192.168.20.125, Foreign port: 1583

Enqueued bytes for transmit: 0, input: 0   mis-ordered: 0 (0 packets)

Timer          Starts    Wakeups             Next(ms)
Retrans            4          0                   0
TimeWait           0          0                   0
SendWnd            0          0                   0
KeepAlive         +5          0             6633000

iss:   10431492   snduna:   10431573   sndnxt:   10431573      sndwnd:      17440
irs: 915717885   rcvnxt: 915717889   rcvwnd:        4380

SRTT: 2812 ms, RXT: 18500 ms, RTV: 4000 ms
minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

Datagrams (max data segment is 1460 bytes):
Rcvd: 5 (out of order: 0), with data: 1, total data bytes: 3
```

```
Sent: 4 (retransmit: 0), with data: 3, total data bytes: 80
```

Related Command

show tcp
show tcp brief

4.2 ACL Configuration Commands

ACL configuration commands include:

- ip access-list
- permit
- deny
- ip access-group
- ipv6 access-group
- show ip access-list

4.2.1 ip access-list

Syntax

To enter the extended IP ACL configuration mode, run the following command.

ip access-list {**standard** | **extended**} *name*

To return to the default setting, use the no form of this command.

no ip access-list {**standard** | **extended**} *name*

Parameters

Parameters	Description
standard	Designates a standard access control list.
extended	Designates an extended access control list.
name	Stands for the name of an access control list. It is a character string with up to 20 characters.

Default Value

No IP access control list is defined by default.

Command Mode

Global configuration mode

Usage Guidelines

This command is used to enter the IP ACL configuration mode and then you can use the deny command and the permit command to configure the access regulation.

Example

The following example shows how to configure a standard IP access control list.

Switch_config# **ip access-list standard** *filter*

Switch_config_std# **deny** *192.168.1.0 255.255.255.0*

Switch_config_std# **permit any**

Related Command

deny

ip access-group

permit

show ip access-list

4.2.2 permit

Syntax

To configure the permission rule in the IP access list, run the following command.

permit { [reverse-mask] *source* [*source-mask*] **| src-range** *source-start source-end* **| any**} [**log | location** *location-id*]*

To return to the default setting, use the no form of this command.

no permit { [reverse-mask] *source* [*source-mask*] **| src-range** *source-start source-end* | **any**} [**log]**

Command under the expansion mode:

permit [reverse-mask] protocol source *source-mask* **destination** *destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**log**] **[offset-zero] [offset-not-zero] [time-range] [ttl] [donotfragment-set] [donotfragment-notset] [is-fragment] [not-fragment]**

no permit [reverse-mask] protocol source *source-mask* **destination** *destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**log**] **[offset-zero] [offset-not-zero] [time-range] [ttl] [donotfragment-set] [donotfragment-notset] [is-fragment] [not-fragment]**

For the Internet Control Message Protocol (ICMP), use the following command syntax.

permit icmp source *source-mask* **destination** *destination-mask* [*icmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**]

For the Internet Group Management Protocol (IGMP), run the following command syntax.

permit igmp source *source-mask* **destination** *destination-mask* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**]

For the Transmission Control Protocol (TCP), use the following command syntax.

permit tcp source *source-mask* [**operator** *port*] **destination** *destination-mask* [**operator** *port*] [**established**] [**precedence** *precedence*] [**tos** tos] [log]

For the User Datagram Protocol (UDP), use the following command syntax.

permit udp source *source-mask* [**operator port** [*port*]] **destination** *destination-mask* [**operator** *port]* [**precedence** *precedence*] [**tos** *tos*] [**log**]

Parameters

Parameters	Description
protocol	Stands for the protocol name or IP protocol number. It can be icmp, igmp, igrp, ip, ospf, tcp or udp, or it can be an integer from 0 to 255 which stands for the IP protocol. To match up any Internet protocol, including ICMP, TCP and UDP, you can use the ip keyword. Some protocols allow further limitations as described below.
source	Stands for a source network or host number. There are two methods to designate the source: 32-bit binary number or a decimal number separated by four points. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
source-mask	Stands for the source address of the network mask. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
destination	Stands for the destination network or host number. There are two methods to designate this parameter: A decimal number separated by four points and a 32-bit binary number. The keyword any is used as the shortened forms of the destination and the destination mask of 0.0.0.0 0.0.0.0.
destination-mask	Stands for the destination address of the network mask. The keyword any is used as the shortened forms of the destination address and the destination mask of 0.0.0.0 0.0.0.0.
precedence *precedence*	(Optional) Filters the packets based on the precedence. The precedence of the packet can be designated by an integer from 0 to 7.
tos *tos*	An optional parameter, meaning that the packets can be filtered

	at the service layer. It is designated by any number between 0 and 15. Its value ranges from 0 to 15.
icmp-type	It is an optional parameter which means that the ICMP packets can be filtered by the ICMP message type. The type is presented by a number between 0 and 255.
igmp-type	It is an optional parameter which means that the ICMP packets can be filtered by the ICMP type or packet name. The type is presented by a number between 0 and 15.
operator	(Optional) Compares the source or destination ports. The operation includes lt (less than), gt(greater than), eq (equal), neq (not equal), src-port range (source port range), dst-port range (destination port range). If the operator symbol is behind source and source-mask, it must match up the source port. If the operator symbol is behind destination and destination-mask, it must match up the destination port.
Port	(Optional) Stands for a decimal number or name of the TCP/UDP port. The port number is a value between 0 and 65535. The name of the TCP port is listed in the Usage Explanation part. When the TCP is filtered, only the name of the TCP port can be used. The names of the UDP ports are also listed in the Usage Explanation part. When the TCP is filtered, only the name of the TCP port can be used. When the UDP is filtered, only the name of the UDP port can be used.
established	An optional parameter for the TCP protocol, representing an established connection. If the TCP data reports that the ACK or RST is configured, the match-up appears. For the unmatched case, the TCP packet is initialized to establish a connection.
reverse-mask	Obtains the reverse mask according to the location.
log	(optional) meaning the logs can be recorded
location	Insert the rule to designated num

Command Mode

IP ACL configuration commands

Usage Guidelines

The virtual terminal path access can be controlled and the content of the routing update can be limited through the transmission of the ACL control packet on the interface. After the matchup occurs, the expanded access control list will not be checked again.

The IP segment, not the initial segment, is received by any extended IP access control list. The extended IP access control list is used to control the virtual terminal's access path or limit the content of the routing update, however, it need not to match up with the source TCP port, the type of the service value or the priority of the packets.

Note:

After an access control list is originally established, (any added content is put at the end of the list.)

The following are the names of the TCP port. For reference of these protocols, see RFC of these protocols. You can search the corresponding port number of these protocols by entering a question mark behind the relative command.

Bgp, ftp, ftp-data, login, pop2, pop3, smtp, telnet and www

The following are the names of the UDP port. For reference of these protocols, see RFC of these protocols. You can search the corresponding port number of these protocols by entering a question mark behind the relative command.

Domain, snmp, syslog, tftp

Example

The following example shows how to allow network segment 192.168.5.0.

Switch_config# **ip access-list standard** *filter*

Switch_config# **permit** *192.168.5.0 255.255.255.0*

Note:

The IP access control list deny ends with a connotative deny regulation.

Related Command

deny

ip access-group

ip access-list

show ip access-list

4.2.3 deny

Syntax

To configure the deny rule in the IP access list configuration mode, run the following command.

deny { [reverse-mask] *source* [*source-mask*] | src-range *source-start source-end* | any} [log | location *location-id*]*

To return to the default setting, use the no form of this command.

no deny { [reverse-mask] *source* [*source-mask*] | **src-range** *source-start source-end* | **any**} [**log**]

Expansion mode is shown below:

deny [reverse-mask] protocol source source-mask destination destination-mask [**precedence** precedence] [**tos** tos] [**log**] **[offset-zero] [offset-not-zero] [time-range] [ttl] [donotfragment-set] [donotfragment-notset] [is-fragment] [not-fragment]**

no deny [reverse-mask] protocol source source-mask destination destination-mask [**precedence** precedence] [**tos** tos] [**log**] **[offset-zero] [offset-not-zero] [time-range] [ttl] [donotfragment-set] [donotfragment-notset] [is-fragment] [not-fragment]**

For the Internet Control Message Protocol (ICMP), use the following command syntax.

deny icmp source source-mask destination destination-mask [icmp-type] [**precedence** precedence] [**tos** tos] [**log**]

For the Internet Group Management Protocol (IGMP), run the following command syntax.

deny igmp source source-mask destination destination-mask [igmp-type] [**precedence** precedence] [**tos** tos] [**log**]

For the Transmission Control Protocol (TCP), use the following command syntax.

deny tcp source source-mask [operator port] destination destination-mask [operator port] [**established**] [**precedence** precedence] [**tos** tos] [**log**]

For the User Datagram Protocol (UDP), use the following command syntax.

deny udp source source-mask [operator port] destination destination-mask [operator port] [**precedence** precedence] [**tos** tos] [**log**]

Parameters

Parameters	Description
protocol	Stands for the protocol name or IP protocol number. It can be icmp, igmp, igrp, ip, ospf, tcp or udp, or it can be an integer from 0 to 255 which stands for the IP protocol. To match up any Internet protocol, including ICMP, TCP and UDP, you can use the ip keyword. Some protocols allow further limitations as described below.
source	Stands for a source network or host number. There are two methods to designate the source: 32-bit binary number or a decimal number separated by four points. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
source-mask	Stands for the source address of the network mask. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
destination	Stands for the destination network or host number. There are two methods to designate this parameter: A decimal number separated by four points and a 32-bit binary number. The keyword any is used as the shortened forms of the destination and the destination mask of 0.0.0.0 0.0.0.0.
destination-mask	Stands for the destination address of the network mask. The keyword any is used as the shortened forms of the destination

	address and the destination mask of 0.0.0.0 0.0.0.0.
precedence *precedence*	(Optional) Filters the packets based on the precedence. The precedence of the packet can be designated by an integer from 0 to 7.
tos *tos*	An optional parameter, meaning that the packets can be filtered at the service layer. It is designated by any number between 0 and 15. Its value ranges from 0 to 15.
icmp-type	It is an optional parameter which means that the ICMP packets can be filtered by the ICMP message type. The type is presented by a number between 0 and 255.
igmp-type	It is an optional parameter which means that the ICMP packets can be filtered by the ICMP type or packet name. The type is presented by a number between 0 and 15.
operator	((Optional) Compares the source or destination ports.) The operation includes lt (less than), gt(greater than), eq (equal), neq (not equal), src-port range (source port range), dst-port range (destination port range). If the operator symbol is behind source and source-mask, it must match up the source port. If the operator symbol is behind destination and destination-mask, it must match up the destination port.
port	(Optional) Stands for a decimal number or name of the TCP/UDP port. The port number is a value between 0 and 65535. The name of the TCP port is listed in the Usage Explanation part. When the TCP is filtered, only the name of the TCP port can be used. The names of the UDP ports are also listed in the Usage Explanation part. When the TCP is filtered, only the name of the TCP port can be used. When the UDP is filtered, only the name of the UDP port can be used.
established	An optional parameter for the TCP protocol, representing an established connection. If the TCP data reports that the ACK or RST is configured, the match-up appears. For the unmatched case, the TCP packet is initialized to establish a connection.
reverse-mask	Obtains the reverse mask according to the location.
log	(optional) meaning the logs can be recorded
location	Insert the rule to designated num

Command Mode

IP ACL configuration commands

Usage Guidelines

The virtual terminal path access can be controlled and the content of the routing update can be limited through the transmission of the ACL control packet on the interface. After the matchup occurs, the expanded access control list will not be checked again. The IP segment, not the initial segment, is received by any extended IP access control list. The extended IP access control list is used to control the virtual terminal's access path or limit the content of the routing update, however, it need not to match up with the source TCP port, the type of the service value or the priority of the packets.

Note:

After an access control list is originally established, any added content is put at the end of the list.

The following are the names of the TCP port. For reference of these protocols, see RFC of these protocols. You can search the corresponding port number of these protocols by entering a question mark behind the relative command.

Bgp, ftp, ftp-data, login, pop2、pop3、smtp、telnet、www

The following are the names of the UDP port. For reference of these protocols, see RFC of these protocols. You can search the corresponding port number of these protocols by entering a question mark behind the relative command.

Domain, snmp,syslog, tftp

Example

The following example shows how to forbid network segment 192.168.5.0.

```
Switch_config# ip access-list standard filter
Switch_config# deny 192.168.5.0 255.255.255.0
```

Note:

The IP access control list ends with a connotative deny regulation.

Related Command

ip access-group
ip access-list
permit
show ip access-list

4.2.4 ip access-group

Syntax

To use it on the vlan interface, run the following command:

[**no**] **ip access-group** *name*{**in** | **out**}

To use it on the physical interface, run the following command:

[**no**] **ip access-group** *name* **[egress]**

To use it in the global mode, run the following command:

[**no**] **ip access-group** *name* **[egress | vlan {***word* **| add** *word* **| remove** *word***} [egress]]**

To configure the access group controlling an interface, run the following command:

Parameters

Parameters	Description
name	Name of the IP access control list
In	The access list is applied in the ingress of the vlan interface.
out	The access list is applied in he egress of the vlan interface.
egress	The access list is applied in the egress of the physical interface.
vlan	The access list is applied in ingress.
Word	Vlan range table
add	Add vlan range table
remove	Delete vlan range table

Command Mode

Global configuration mode, interface configuration mode and vlan interface configuration mode

Usage Guidelines

The access control list can be used on the incoming or outgoing interface. After a packet is received, the source address of the packet will be checked according to the standard egress interface access control list. For the expanded access control list, the OLT also checks the destination address.

For the access list applied on vlan interface, if the access list allows the packet, the software continues to handle the packet. However, if the access control list forbids the destination packet, the system will drop the packet and then returns an ICMP unreachable packet.

Most rules in the ACL (which applies on the global and physical interface) take effect through hardware; those that hardware does not support give no errors but they have no actual effects; a few rules such as time-range take effect through software.

Note:

The IPv4 standard ACL supports the following rules:

any: means any source IP address.

source-addr source-mask: means matching up the source address.

reverse-mask source-addr source-mask: means to use the reverse source address for match-up.

The IPv4 extended ACL supports the following rules:

any: means any IP address.

ip-protocol: means the IP protocol ID.

ip-addr ip-mask: means IP address match-up.

Interface interface-id: means layer-3 interface match-up.

eq/gt/lt/src-portrange: means TCP/UDP port ID match-up.

established/tos/is-fragment/not-fragment/precedence/ttl/offset-not-zero/offset-zero/donotfragment-set/ donotfragment-notset/*icmp-type*: means field match-up, among which ttl must be set to equal.

Example

The following example shows how to apply the filter list on the egress port of Ethernet interface g0/1:

```
Switch_config# interface GigaEthernet 1/1
Switch_config_g0/1# ip access-group filter egress
```

Related Command

ip access-list

show ip access-list

4.2.5 ipv6 access-group

Syntax

To use the function on the vlan interface, run the following command.

To use the function on the physical interface, run the following command.

[**no**] **ipv6 access-group** *name*{**in** | **out**}

To use the function in the global mode, run the following command.

[**no**] **ipv6 access-group** *name* **[egress]**

To configure the access group controlling an interface, run the following command.

[**no**] **ipv6 access-group** *name* **[egress | vlan {***word* **| add** *word* **| remove** *word***}]**

Parameters

Parameters	Description
name	Name of the IP access control list

in	The access list is applied in the ingress of the vlan interface.
out	The access list is applied in the egress of the vlan interface.
egress	The access list is applied in the egress of the physical interface.
vlan	The access list is applied in ingress.
Word	Vlan range table
add	Add vlan range table
remove	Delete vlan range table

Command Mode

Global configuration mode, interface configuration mode, VLAN interface configuration mode

Usage Guidelines

Most rules in the ACL take effect through hardware; those that hardware does not support give no errors but they have no actual effects; a few rules such as time-range take effect through software.

Note:

The IPv6 ACL supports the following rules:

any: means any IP address.

Ipv6-addr/ host *Ipv6-addr:* means IPv6 address match-up.

ip-protocol: means the IPv6 protocol ID.

eq/gt/lt/src-portrange: means TCP/UDP port ID match-up.

dscp/flow-label: means field match-up.

Example

The following example shows how to apply the ACL filter at the ingress direction of interface g0/1.

```
Switch_config# inter g0/1
Switch_config_g0/1# ipv6 access-group filter
```

4.2.6 show ip access-list

Syntax

To show the current IP access list content, run the following command.

show ip access-list[*access-list-name*]

Parameters

Parameters	Description
access-list-name	Stands for the name of an access control list. It is a character string with up to 20 characters.

Default Value

This command is used to display all standard and extended IP access control lists.

Command Mode

Other modes except the user mode

Usage Guidelines

The command helps you to designate a specific access control list.

Example

The following information is displayed when the show ip access-list command is run in case an IP access control list is designated.

```
Switch# show ip access-list
ip access-list standard aaa
permit 192.2.2.1
permit 192.3.3.0 255.255.255.0
ip access-list extended bbb
permit tcp any any eq www
permit ip any any
```

The following information is displayed when the show ip access-lists bbb command is run in case that an access control list is designated.

```
Switch# show ip access-list bbb
ip access-list extended bbb
permit tcp any any eq www
permit ip any any
```